Dell Networking Command Line Reference Guide for the MXL 10/40GbE Switch I/O Module

9.5(0.1)

Notes, Cautions, and Warnings

NOTE: A NOTE indicates important information that helps you make better use of your computer.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Copyright © 2014 Dell Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. Dell™ and the Dell logo are trademarks of Dell Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

2014 - 07

Rev. A00

Contents

1 About this Guide.. 48

Objectives...48

Audience...49

Conventions...49

Information Icons...49

2 CLI Basics.. 50

Accessing the Command Line..50

Multiple Configuration Users..50

Navigating the CLI.. 51

Obtaining Help..51

Using the Keyword no Command..53

Filtering show Commands...53

Command Modes.. 54

3 File Management.. 59

cd...59

copy...59

copy running-config startup-config... 61

delete.. 61

format flash...62

HTTP Copy via CLI...63

logging coredump..63

logging coredump server..64

pwd...65

rename...65

show boot system...66

show file..66

show file-systems..67

show os-version..68

show running-config...69

show startup-config..72

show version..73

upgrade boot..74

upgrade system.. 75

verify...76

4 Control and Monitoring.. 78

asset-tag....78
asf-mode....78
banner exec....79
banner login....80
banner motd....81
clear alarms....82
clear command history....82
clear line....82
configure....83
debug cpu-traffic-stats....83
debug ftpserver....84
disable....84
do....85
enable....85
enable optic-info-update interval....86
end....87
exec-banner....87
exec-timeout....88
exit....88
ftp-server enable....89
ftp-server topdir....90
ftp-server username....90
hostname....91
ip ftp password....91
ip ftp source-interface....92
ip ftp username....93
ip telnet server enable....93
ip telnet source-interface....93
ip tftp source-interface....94
line....95
motd-banner....95
ping....96
reload....98
send....98
service timestamps....99
show alarms....100
show command-history....100
show command-tree....102
show cpu-traffic-stats....103
show debugging....104
show environment....104
show inventory....105

show memory.. 107
show processes cpu..107
show processes ipc flow-control..111
show processes memory... 112
show software ifm... 114
show system.. 115
show tech-support... 117
telnet...120
terminal xml... 121
traceroute..121
undebug all.. 123
virtual-ip..123
write.. 123

5 802.1X.. 125
debug dot1x...125
dot1x auth-fail-vlan...126
dot1x auth-server.. 127
dot1x auth-type mab-only..127
dot1x authentication (Configuration)...128
dot1x authentication (Interface).. 128
dot1x guest-vlan..128
dot1x host-mode... 129
dot1x mac-auth-bypass...130
dot1x max-eap-req..130
dot1x max-supplicants.. 131
dot1x port-control... 131
dot1x quiet-period...132
dot1x reauthentication...132
dot1x reauth-max..133
dot1x server-timeout...133
dot1x supplicant-timeout.. 134
dot1x tx-period..134
show dot1x cos-mapping interface..135
show dot1x interface...136

6 Access Control Lists (ACL)..140
Commands Common to all ACL Types..140
description..140
remark.. 141
resequence access-list.. 142
resequence prefix-list ipv4.. 142

show config....143
Common IP ACL Commands....143
access-class....144
clear counters ip access-group....144
ip access-group....144
show ip access-lists....145
show ip accounting access-list....146
Standard IP ACL Commands....147
deny (for Standard IP ACLs)....147
ip access-list standard....149
permit (for Standard IP ACLs)....150
seq....152
Extended IP ACL Commands....154
deny (for Extended IP ACLs)....155
deny icmp....157
deny tcp....159
deny udp....162
ip access-list extended....165
permit (for Extended IP ACLs)....166
permit icmp....168
permit tcp....170
permit udp....174
seq....177
Common MAC Access List Commands....180
clear counters mac access-group....180
mac access-group....180
show mac access-lists....182
show mac accounting access-list....182
Standard MAC ACL Commands....183
deny....183
mac access-list standard....185
permit....186
seq....188
Extended MAC ACL Commands....190
deny....190
mac access-list extended....191
permit....192
seq....194
IP Prefix List Commands....195
clear ip prefix-list....195
deny....195
ip prefix-list....196

permit....197
seq....197
show config....198
show ip prefix-list detail....199
show ip prefix-list summary....199
Route Map Commands....200
continue....200
description....201
match interface....202
match ip address....202
match ip next-hop....203
match ip route-source....204
match metric....205
match route-type....205
match tag....206
route-map....207
set automatic-tag....207
set metric....208
set metric-type....209
set tag....209
show config....210
show route-map....210
deny (for Standard IP ACLs)....211
deny (for Extended IP ACLs)....213
seq....215
deny tcp....217
deny udp....221
deny arp (for Extended MAC ACLs)....223
deny icmp....226
deny ether-type (for Extended MAC ACLs)....228
deny....231
deny....232
permit (for Standard IP ACLs)....235
permit arp....237
permit ether-type (for Extended MAC ACLs)....239
permit icmp....242
permit udp....245
permit (for Extended IP ACLs)....248
permit....250
seq....252
permit tcp....254
seq arp....257

seq ether-type.................... 260
seq.................... 263
seq.................... 266
permit udp.................... 269
permit tcp.................... 271
permit icmp.................... 274
permit.................... 276
deny udp (for IPv6 ACLs).................... 277
deny tcp (for IPv6 ACLs).................... 279
deny icmp (for Extended IPv6 ACLs).................... 282
deny (for IPv6 ACLs).................... 284

7 Access Control List (ACL) VLAN Groups and Content Addressable Memory (CAM).................... 286
member vlan.................... 286
ip access-group.................... 287
show acl-vlan-group 287
show cam-acl-vlan.................... 289
cam-acl-vlan.................... 290
show cam-usage.................... 291
show running config acl-vlan-group.................... 294
acl-vlan-group.................... 295
show acl-vlan-group detail.................... 296
description (ACL VLAN Group).................... 297

8 Bidirectional Forwarding Detection (BFD).................... 298
bfd all-neighbors.................... 298
bfd disable.................... 299
bfd enable (Configuration).................... 300
bfd enable (Interface).................... 300
bfd interval 300
bfd neighbor.................... 301
bfd protocol-liveness.................... 302
ip route bfd.................... 302
ipv6 ospf bfd all-neighbors.................... 303
isis bfd all-neighbors.................... 304
neighbor bfd.................... 305
neighbor bfd disable.................... 306
show bfd neighbors.................... 307
vrrp bfd neighbor.................... 309

9 Border Gateway Protocol IPv4 (BGPv4).................... 310

BGPv4 Commands........310
address-family........310
aggregate-address........311
bgp add-path........312
bgp always-compare-med........313
bgp asnotation........313
bgp bestpath as-path ignore........314
bgp bestpath as-path multipath-relax........315
bgp bestpath med confed........315
bgp bestpath med missing-as-best........316
bgp bestpath router-id ignore........316
bgp client-to-client reflection........317
bgp cluster-id........317
bgp confederation identifier........318
bgp confederation peers........319
bgp dampening........319
bgp default local-preference........321
bgp enforce-first-as........321
bgp fast-external-failover........322
bgp four-octet-as-support........322
bgp graceful-restart........323
bgp non-deterministic-med........324
bgp recursive-bgp-next-hop........324
bgp regex-eval-optz-disable........325
bgp router-id........326
bgp soft-reconfig-backup........326
capture bgp-pdu neighbor........327
capture bgp-pdu max-buffer-size........328
clear ip bgp........328
clear ip bgp dampening........329
clear ip bgp flap-statistics........329
clear ip bgp peer-group........330
debug ip bgp........331
debug ip bgp dampening........332
debug ip bgp events........332
debug ip bgp keepalives........333
debug ip bgp notifications........334
debug ip bgp soft-reconfiguration........334
debug ip bgp updates........335
default-metric........336
description........336
max-paths........337

neighbor activate.......... 337
neighbor add-path.......... 338
neighbor advertisement-interval.......... 339
neighbor advertisement-start.......... 339
neighbor allowas-in.......... 340
neighbor default-originate.......... 341
neighbor description.......... 341
neighbor distribute-list.......... 342
neighbor ebgp-multihop.......... 343
neighbor fall-over.......... 343
neighbor graceful-restart.......... 344
neighbor local-as.......... 345
neighbor maximum-prefix.......... 345
neighbor password.......... 346
neighbor peer-group (assigning peers).......... 347
neighbor peer-group (creating group).......... 348
neighbor peer-group passive.......... 349
neighbor remote-as.......... 350
neighbor remove-private-as.......... 351
neighbor route-map.......... 351
neighbor route-reflector-client.......... 352
neighbor shutdown.......... 353
neighbor soft-reconfiguration inbound.......... 354
neighbor timers.......... 355
neighbor update-source.......... 355
neighbor weight.......... 356
network.......... 357
network backdoor.......... 358
redistribute.......... 358
redistribute ospf.......... 359
router bgp.......... 360
show capture bgp-pdu neighbor.......... 361
show config.......... 362
show ip bgp.......... 362
show ip bgp cluster-list.......... 364
show ip bgp community.......... 365
show ip bgp community-list.......... 368
show ip bgp dampened-paths.......... 369
show ip bgp detail.......... 369
show ip bgp extcommunity-list.......... 371
show ip bgp filter-list.......... 372
show ip bgp flap-statistics.......... 373

show ip bgp inconsistent-as....375
show ip bgp neighbors....376
show ip bgp next-hop....381
show ip bgp paths....382
show ip bgp paths as-path....383
show ip bgp paths community....384
show ip bgp peer-group....385
show ip bgp regexp....387
show ip bgp summary....389
show running-config bgp....391
timers bgp....392
MBGP Commands....392
debug ip bgp dampening....392
distance bgp....393
show ip bgp dampened-paths....394
BGP Extended Communities (RFC 4360)....394
set extcommunity rt....395
set extcommunity soo....396
show ip bgp paths extcommunity....397
show ip bgp extcommunity-list....397
IPv6 BGP Commands....398
bgp soft-reconfig-backup....398
clear ip bgp ipv6 unicast soft....399
debug ip bgp ipv6 unicast soft-reconfiguration....400
ipv6 prefix-list....400
show ipv6 prefix-list....401
IPv6 MBGP Commands....401
show ipv6 mbgproutes....401

10 Content Addressable Memory (CAM)....403
CAM Profile Commands....403
cam-acl (Configuration)....403
cam-optimization....406
show cam-acl....406
show cam-acl-egress....408

11 Control Plane Policing (CoPP)....409
control-plane-cpuqos....409
service-policy rate-limit-cpu-queues....409
service-policy rate-limit-protocols....410
show cpu-queue rate cp....410
show ip protocol-queue-mapping....411

show ipv6 protocol-queue-mapping.......... 412
show mac protocol-queue-mapping.......... 413

12 Data Center Bridging (DCB).......... 414

advertise dcbx-appln-tlv.......... 414
advertise dcbx-tlv.......... 415
bandwidth-percentage.......... 415
dcb-enable.......... 416
dcb-input.......... 417
dcb-output.......... 418
dcb-policy buffer-threshold (Global Configuration).......... 419
dcb-policy buffer-threshold (Interface Configuration).......... 419
dcb-policy input.......... 420
dcb-policy input stack-unit stack-ports all.......... 421
dcb-policy output.......... 422
dcb-policy output stack-unit stack-ports all.......... 423
dcb stack-unit all pfc-buffering pfc-port-count pfc-queues.......... 424
dcb stack-unit pfc-buffering pfc-port-count pfc-queues.......... 424
dcbx port-role.......... 425
dcbx version.......... 426
debug dcbx.......... 427
description.......... 428
ets mode on.......... 428
fcoe priority-bits.......... 429
iscsi priority-bits.......... 430
priority.......... 430
pfc link-delay.......... 432
pfc mode on.......... 432
pfc no-drop queues.......... 433
pfc priority.......... 434
priority-group.......... 435
priority-group qos-policy.......... 436
priority-list.......... 437
qos-policy-output ets.......... 437
scheduler.......... 438
set-pgid.......... 439
show dcb.......... 440
show interface dcbx detail.......... 440
show interface ets.......... 443
show interface pfc.......... 447
show interface pfc statistics.......... 450
show qos dcb-input.......... 450

show qos dcb-output........ 451
show qos priority-groups........ 452
show stack-unit stack-ports ets details........ 452
dcb pfc-shared-buffer-size........ 453
dcb-buffer-threshold 454
dcb enable pfc-queues........ 455
dcb <ets | pfc> enable........ 455
dcb-policy buffer-threshold (Interface Configuration)........ 456
dcb-policy buffer-threshold (Global Configuration)........ 457
pfc mode on........ 458
priority-pgid........ 458
qos-policy-buffer........ 460
show qos dcb-map........ 462
show stack-unit stack-ports pfc details........ 463

13 Debugging and Diagnostics........ 464
Offline Diagnostic Commands........ 464
diag stack-unit........ 464
offline stack-unit........ 465
online stack-unit........ 466
Buffer Tuning Commands........ 466
buffer (Buffer Profile)........ 466
buffer (Configuration)........ 468
buffer-profile (Configuration)........ 469
buffer-profile (Interface)........ 470
show buffer-profile........ 470
show buffer-profile interface........ 471
Hardware Commands........ 472
clear hardware stack-unit........ 472
clear hardware system-flow........ 473
show hardware layer2 acl........ 473
show hardware layer3........ 474
show hardware stack-unit........ 474
show hardware system-flow........ 480

14 Dynamic Host Configuration Protocol (DHCP)........ 484
Commands to Configure the System to be a DHCP Server........ 484
clear ip dhcp........ 484
debug ip dhcp server........ 485
default-router........ 485
disable........ 486
dns-server........ 486

domain-name....486
excluded-address....487
hardware-address....487
host....488
lease....488
netbios-name-server....488
netbios-node-type....489
network....489
show ip dhcp binding....490
show ip dhcp configuration....490
show ip dhcp conflict....490
show ip dhcp server....491
Commands to Configure the System to be a DHCP Client....491
ip address dhcp....491
Other Commands Supported by the DHCP Client....492
clear ip dhcp client statistics....492
debug ip dhcp clients events....493
debug ip dhcp clients packets....493
release dhcp interface....494
renew dhcp interface....494
show ip dhcp client statistics....495
show ip dhcp lease....496
Commands to Configure Secure DHCP....496
arp inspection....496
arp inspection-trust....497
clear ip dhcp snooping....497
ip dhcp snooping....497
ip dhcp snooping database....498
ip dhcp snooping binding....498
ip dhcp snooping database renew....499
ip dhcp snooping trust....499
ip dhcp source-address-validation....500
ip dhcp snooping vlan....500
ip dhcp relay....501
show ip dhcp snooping....501
ip dhcp snooping verify mac-address....502

15 Equal Cost Multi-Path (ECMP)....503
ecmp-group....503
hash-algorithm....504
hash-algorithm ecmp....506
hash-algorithm seed....507

ip ecmp-group........ 508
link-bundle-distribution trigger-threshold........ 508
link-bundle-monitor enable........ 509
show config........ 509
show link-bundle distribution........ 510

16 FIPS Cryptography........ 511
fips mode enable........ 511
show fips status........ 511
show ip ssh........ 512
ssh........ 513

17 FIP Snooping........ 515
clear fip-snooping database interface vlan........ 515
clear fip-snooping statistics........ 516
clear fip-snooping statistics........ 516
feature fip-snooping........ 517
fip-snooping enable........ 517
fip-snooping fc-map........ 518
fip-snooping port-mode fcf........ 518
show fip-snooping config........ 519
show fip-snooping enode........ 519
show fip-snooping fcf........ 520
show fip-snooping sessions........ 521
show fip-snooping statistics........ 522
show fip-snooping system........ 525
show fip-snooping vlan........ 525

18 Force10 Resilient Ring Protocol (FRRP)........ 527
clear frrp........ 527
debug frrp........ 528
description........ 529
disable........ 529
interface........ 529
member-vlan........ 530
mode........ 531
protocol frrp........ 531
show frrp........ 532
timer........ 533

19 GARP VLAN Registration (GVRP)........ 535
clear gvrp statistics........ 536

debug gvrp.......... 536
disable.......... 537
garp timers.......... 538
gvrp enable.......... 539
gvrp registration.......... 539
protocol gvrp.......... 540
show config.......... 540
show garp timers.......... 540
show gvrp.......... 541
clear gvrp statistics.......... 542
show vlan.......... 543

20 Internet Group Management Protocol (IGMP).......... 545
IGMP Snooping Commands.......... 545
ip igmp access-group.......... 546
ip igmp group-join-limit.......... 546
ip igmp querier-timeout.......... 547
ip igmp query-interval.......... 547
ip igmp query-max-resp-time.......... 548
ip igmp version.......... 548
ip igmp snooping enable.......... 548
ip igmp snooping fast-leave.......... 549
ip igmp snooping flood.......... 549
ip igmp snooping last-member-query-interval.......... 550
ip igmp snooping mrouter.......... 550
ip igmp snooping querier.......... 551
show ip igmp snooping mrouter.......... 552

21 Interfaces.......... 553
Basic Interface Commands.......... 553
clear counters.......... 553
clear dampening.......... 554
cx4-cable-length.......... 555
dampening.......... 556
description.......... 557
duplex (1000/10000 Interfaces).......... 558
flowcontrol.......... 559
interface.......... 561
interface loopback.......... 562
interface ManagementEthernet.......... 563
interface null.......... 564
interface range.......... 564

interface range macro (define)....567
interface range macro name....568
interface vlan....569
intf-type cr4 autoneg....569
keepalive....570
monitor interface....571
mtu....572
negotiation auto....574
portmode hybrid....576
rate-interval....578
show config....578
show config (from INTERFACE RANGE mode)....579
show interfaces....579
show interfaces configured....584
show interfaces dampening....585
show interfaces description....586
show interfaces stack-unit....587
show interfaces status....588
show interfaces switchport....589
show interfaces transceiver....591
show range....596
shutdown....596
speed (for 1000/10000/auto interfaces)....597
stack-unit portmode....598
Port Channel Commands....599
channel-member....599
group....601
interface port-channel....602
minimum-links....603
port-channel failover-group....603
show config....604
show interfaces port-channel....604
Time Domain Reflectometer (TDR)....607
tdr-cable-test....607
show tdr....608
UDP Broadcast....609
debug ip udp-helper....609
ip udp-broadcast-address....610
ip udp-helper udp-port....610
show ip udp-helper....611
Enhanced Validation of Interface Ranges....612

22 IPv4 Routing......613
arp......613
arp learn-enable......614
arp retries......614
arp timeout......615
clear arp-cache......615
clear host......616
clear ip fib stack-unit......616
clear ip route......617
clear tcp statistics......617
debug arp......618
debug ip dhcp......618
debug ip icmp......619
debug ip packet......620
ip address......623
ip directed-broadcast......623
ip domain-list......624
ip domain-lookup......625
ip domain-name......625
ip helper-address......626
ip helper-address hop-count disable......627
ip host......627
ip icmp source-interface......628
ipv6 icmp source-interface......629
ip max-frag-count......630
ip name-server......631
ip proxy-arp......631
ip route......632
ip source-route......633
ip tcp initial-time......633
show ip tcp initial-time......634
ip unreachables......634
management route......635
show arp......635
show arp retries......638
show hosts......638
show ip cam stack-unit......640
show ip fib stack-unit......642
show ip interface......643
show ip management-route......645
show ip protocols......646

show ip route....................646
show ip route list....................649
show ip route summary....................650
show ip traffic....................651
show tcp statistics....................653

23 Internet Protocol Security (IPSec)....................656
crypto ipsec transform-set....................656
crypto ipsec policy....................658
management crypto-policy....................658
match....................659
session-key....................660
show crypto ipsec transform-set....................660
show crypto ipsec policy....................661
transform-set....................663

24 IPv6 Access Control Lists (IPv6 ACLs)....................664
IPv6 ACL Commands....................664
cam-acl....................664
cam-acl-egress....................665
ipv6 access-list....................666
ipv6 control-plane egress-filter....................667
permit....................667
permit icmp....................669
show cam-acl....................671
show cam-acl-egress....................672

25 IPv6 Basics....................673
clear ipv6 fib....................673
clear ipv6 route....................673
clear ipv6 mld_host....................674
ipv6 address autoconfig....................674
ipv6 address....................675
ipv6 address eui64....................676
ipv6 control-plane icmp error-rate-limit....................676
ipv6 flowlabel-zero....................677
ipv6 host....................677
ipv6 name-server....................678
ipv6 nd dad attempts....................678
ipv6 nd dns-server 679
ipv6 nd prefix....................680
ipv6 route....................681

ipv6 unicast-routing........683
show ipv6 cam stack-unit........683
show ipv6 control-plane icmp........684
show ipv6 fib stack-unit........684
show ipv6 flowlabel-zero........685
show ipv6 interface........685
show ipv6 mld_host........688
show ipv6 route........689
trust ipv6-diffserv........691

26 IPv6 Border Gateway Protocol (IPv6 BGP)........693

IPv6 BGP Commands........693
address family........693
aggregate-address........694
bgp always-compare-med........695
bgp bestpath as-path ignore........696
bgp bestpath med confed........696
bgp bestpath med missing-as-best........697
bgp client-to-client reflection........697
bgp cluster-id........698
bgp confederation identifier........698
bgp confederation peers........699
bgp dampening........700
bgp default local-preference........701
bgp enforce-first-as........701
bgp fast-external-fallover........702
bgp four-octet-as-support........702
bgp graceful-restart........703
bgp log-neighbor-changes........704
bgp non-deterministic-med........704
bgp recursive-bgp-next-hop........705
bgp regex-eval-optz-disable........705
bgp router-id........706
bgp soft-reconfig-backup........706
capture bgp-pdu neighbor (ipv6)........707
capture bgp-pdu max-buffer-size........708
clear ip bgp * (asterisk)........708
clear ip bgp as-number........709
clear ip bgp ipv6-address........710
clear ip bgp peer-group........711
clear ip bgp ipv6 dampening........711
clear ip bgp ipv6 flap-statistics........712

clear ip bgp ipv6 unicast soft.......713
debug ip bgp.......713
debug ip bgp events.......714
debug ip bgp ipv6 dampening.......715
debug ip bgp ipv6 unicast soft-reconfiguration.......716
debug ip bgp keepalives.......716
debug ip bgp notifications.......717
debug ip bgp updates.......718
default-metric.......719
description.......719
distance bgp.......720
maximum-paths.......720
neighbor activate.......721
neighbor advertisement-interval.......722
neighbor allowas-in.......722
neighbor default-originate.......723
neighbor description.......724
neighbor distribute-list.......724
neighbor ebgp-multihop.......725
neighbor fall-over.......726
neighbor filter-list.......726
neighbor maximum-prefix.......727
neighbor X:X:X::X password.......728
neighbor next-hop-self.......729
neighbor peer-group (assigning peers).......729
neighbor peer-group (creating group).......730
neighbor peer-group passive.......731
neighbor remote-as.......732
neighbor remove-private-as.......732
neighbor route-map.......733
neighbor route-reflector-client.......734
neighbor send-community.......735
neighbor shutdown.......735
neighbor soft-reconfiguration inbound.......736
neighbor subnet.......737
neighbor timers.......737
neighbor update-source.......738
neighbor weight.......739
network.......739
network backdoor.......740
redistribute.......741
redistribute isis.......742

redistribute ospf......742
router bgp......743
show capture bgp-pdu neighbor......744
show config......744
show ip bgp ipv6 unicast......745
show ip bgp ipv6 unicast cluster-list......745
show ip bgp ipv6 unicast community......746
show ip bgp ipv6 unicast community-list......747
show ip bgp ipv6 unicast dampened-paths......747
show ip bgp ipv6 unicast detail......747
show ip bgp ipv6 unicast extcommunity-list......748
show ip bgp ipv6 unicast filter-list......748
show ip bgp ipv6 unicast flap-statistics......749
show ip bgp ipv6 unicast inconsistent-as......749
show ip bgp ipv6 unicast neighbors......750
show ip bgp ipv6 unicast peer-group......753
show ip bgp ipv6 unicast summary......754
show ip bgp next-hop......755
show ip bgp paths......756
show ip bgp paths as-path......756
show ip bgp paths community......757
show ip bgp paths extcommunity......757
show ip bgp regexp......757
timers bgp......758
IPv6 MBGP Commands......759
address family......759
aggregate-address......759
bgp dampening......761
clear ip bgp ipv6 unicast......761
clear ip bgp ipv6 unicast dampening......762
clear ip bgp ipv6 unicast flap-statistics......762
debug ip bgp ipv6 unicast dampening......763
debug ip bgp ipv6 unicast peer-group updates......763
debug ip bgp ipv6 unicast updates......764
distance bgp......765
neighbor activate......765
neighbor advertisement-interval......766
neighbor default-originate......767
neighbor distribute-list......767
neighbor filter-list......768
neighbor maximum-prefix......769
neighbor next-hop-self......770

neighbor remove-private-as......770
neighbor route-map......771
neighbor route-reflector-client......772
network......772
redistribute......773
show ip bgp ipv6 unicast......774
show ip bgp ipv6 unicast cluster-list......774
show ip bgp ipv6 unicast community......775
show ip bgp ipv6 unicast community-list......776
show ip bgp ipv6 unicast dampened-paths......776
show ip bgp ipv6 unicast detail......776
show ip bgp ipv6 unicast filter-list......777
show ip bgp ipv6 unicast flap-statistics......777
show ip bgp ipv6 unicast inconsistent-as......779
show ip bgp ipv6 unicast neighbors......779
show ip bgp ipv6 unicast peer-group......782
show ip bgp ipv6 unicast summary......783

27 iSCSI Optimization......785

advertise dcbx-app-tlv......785
iscsi aging time......785
iscsi cos......786
iscsi enable......787
iscsi priority-bits......787
iscsi profile-compellant......788
iscsi target port......788
show iscsi......789
show iscsi session......790
show iscsi session detailed......790
show run iscsi......791

28 Intermediate System to Intermediate System (IS-IS)......792

adjacency-check......792
advertise......793
area-password......793
clear config......794
clear isis......795
clns host......795
debug isis......796
debug isis adj-packets......796
debug isis local-updates......797
debug isis snp-packets......797

debug isis spf-triggers.......... 798
debug isis update-packets.......... 798
default-information originate.......... 799
description.......... 800
distance.......... 800
distribute-list in.......... 801
distribute-list out.......... 802
distribute-list redistributed-override.......... 802
domain-password.......... 803
graceful-restart ietf.......... 804
graceful-restart interval.......... 804
graceful-restart t1.......... 805
graceful-restart t2.......... 805
graceful-restart t3.......... 806
graceful-restart restart-wait.......... 806
hello padding.......... 807
hostname dynamic.......... 808
ignore-lsp-errors.......... 808
ip router isis.......... 809
ipv6 router isis.......... 809
isis circuit-type.......... 810
isis csnp-interval.......... 811
isis csnp-interval.......... 811
isis hello-multiplier.......... 812
isis hello padding.......... 813
isis ipv6 metric.......... 813
isis metric.......... 814
isis network point-to-point.......... 814
isis password.......... 815
isis priority.......... 816
is-type.......... 816
log-adjacency-changes.......... 817
lsp-gen-interval.......... 817
lsp-mtu.......... 818
lsp-refresh-interval.......... 819
max-area-addresses.......... 820
max-lsp-lifetime.......... 820
maximum-paths.......... 821
metric-style.......... 821
multi-topology.......... 822
net.......... 823
passive-interface.......... 823

redistribute......824
redistribute bgp......825
redistribute ospf......827
router isis......828
set-overload-bit......829
show config......829
show isis database......830
show isis graceful-restart detail......833
show isis hostname......833
show isis interface......834
show isis neighbors......835
show isis protocol......836
show isis traffic......837
spf-interval......838

29 Link Aggregation Control Protocol (LACP)...... 840
clear lacp counters......840
debug lacp......840
lacp long-timeout......841
lacp port-priority......842
lacp system-priority......842
port-channel mode......843
port-channel-protocol lacp......844
show lacp......844

30 Layer 2......846
MAC Addressing Commands......846
clear mac-address-table......846
mac-address-table aging-time......847
mac-address-table static......847
mac-address-table station-move refresh-arp......848
mac learning-limit......848
mac learning-limit learn-limit-violation......850
mac learning-limit station-move-violation......850
mac learning-limit reset......851
show cam mac stack-unit......851
show mac-address-table......852
show mac-address-table aging-time......855
show mac learning-limit......856
Virtual LAN (VLAN) Commands......856
description......857
default vlan-id......857

default-vlan disable........ 858
name........ 858
show config........ 859
show vlan........ 859
tagged........ 861
track ip........ 862
untagged........ 863

31 Link Layer Discovery Protocol (LLDP)........ 865

advertise dot1-tlv........ 865
advertise dot3-tlv........ 866
advertise management-tlv........ 866
clear lldp counters........ 867
clear lldp neighbors........ 868
debug lldp interface........ 868
disable........ 869
hello........ 870
mode........ 870
multiplier........ 871
protocol lldp (Configuration)........ 871
protocol lldp (Interface)........ 872
show lldp neighbors........ 872
show lldp statistics........ 873
show running-config lldp........ 873
LLDP-MED Commands........ 874
advertise med guest-voice........ 874
advertise med guest-voice-signaling........ 875
advertise med location-identification........ 876
advertise med power-via-mdi........ 877
advertise med softphone-voice........ 877
advertise med streaming-video........ 878
advertise med video-conferencing........ 878
advertise med voice-signaling........ 879
advertise med voice........ 880
advertise med voice-signaling........ 880

32 Microsoft Network Load Balancing........ 882

mac-address-table static (for Multicast MAC Address)........ 884
ip vlan-flooding........ 886

33 Multicast Source Discovery Protocol (MSDP)........ 887

clear ip msdp peer........ 887

clear ip msdp sa-cache.......... 887
clear ip msdp statistic.......... 888
debug ip msdp.......... 888
ip msdp cache-rejected-sa.......... 889
ip msdp default-peer.......... 889
ip msdp log-adjacency-changes.......... 890
ip msdp mesh-group.......... 890
ip msdp originator-id.......... 891
ip msdp peer.......... 892
ip msdp redistribute.......... 893
ip msdp sa-filter.......... 893
ip msdp sa-limit.......... 894
ip msdp shutdown.......... 895
ip multicast-msdp.......... 895
show ip msdp.......... 895
show ip msdp sa-cache rejected-sa.......... 896

34 Multiple Spanning Tree Protocol (MSTP).......... 898
debug spanning-tree mstp.......... 898
description.......... 899
disable.......... 899
disable.......... 900
forward-delay.......... 900
hello-time.......... 901
max-age.......... 901
max-hops.......... 902
msti.......... 902
name.......... 903
protocol spanning-tree mstp.......... 904
revision.......... 904
show config.......... 905
show spanning-tree mst configuration.......... 905
show spanning-tree msti.......... 906
spanning-tree.......... 908
spanning-tree msti.......... 909
spanning-tree mstp.......... 909
tc-flush-standard.......... 910

35 Multicast.......... 912
IPv4 Multicast Commands.......... 912
clear ip mroute.......... 912
ip mroute.......... 913

ip multicast-limit....914
ip multicast-routing....914
show ip mroute....915
show ip rpf....917
IPv6 Multicast Commands....918
debug ipv6 mld_host....918
ip multicast-limit....919

36 Neighbor Discovery Protocol (NDP)....920

clear ipv6 neighbors....920
ipv6 neighbor....921
show ipv6 neighbors....922

37 Open Shortest Path First (OSPFv2 and OSPFv3)....924

OSPFv2 Commands....924
area default-cost....924
area nssa....925
area range....926
area stub....926
auto-cost....927
clear ip ospf....927
clear ip ospf statistics....928
debug ip ospf....929
default-information originate....931
default-metric....932
description....932
distance....933
distance ospf....933
distribute-list in....934
distribute-list out....935
fast-convergence....935
flood-2328....936
graceful-restart grace-period....937
graceful-restart helper-reject....937
graceful-restart mode....938
graceful-restart role....938
ip ospf auth-change-wait-time....939
ip ospf authentication-key....939
ip ospf cost....940
ip ospf dead-interval....940
ip ospf hello-interval....941
ip ospf message-digest-key....941

ip ospf mtu-ignore....................942
ip ospf network....................942
ip ospf priority....................943
ip ospf retransmit-interval....................943
ip ospf transmit-delay.................... 944
log-adjacency-changes....................944
maximum-paths.................... 945
mib-binding.................... 945
network area....................946
passive-interface....................947
redistribute....................948
redistribute bgp....................949
redistribute isis....................950
router-id.................... 951
router ospf.................... 951
show config....................952
show ip ospf....................952
show ip ospf asbr....................953
show ip ospf database....................954
show ip ospf database asbr-summary....................956
show ip ospf database external....................958
show ip ospf database network....................960
show ip ospf database nssa-external....................962
show ip ospf database opaque-area.................... 962
show ip ospf database opaque-as....................964
show ip ospf database opaque-link....................965
show ip ospf database router....................965
show ip ospf database summary.................... 968
show ip ospf interface.................... 970
show ip ospf neighbor.................... 972
show ip ospf routes....................973
show ip ospf statistics.................... 973
show ip ospf timers rate-limit....................977
show ip ospf topology.................... 977
summary-address.................... 978
timers spf....................979
timers throttle lsa all.................... 979
timers throttle lsa arrival....................980
OSPFv3 Commands.................... 981
area authentication.................... 981
area encryption....................982
clear ipv6 ospf process....................984

debug ipv6 ospf bfd....984
debug ipv6 ospf....986
default-information originate....986
graceful-restart grace-period....987
graceful-restart mode....988
ipv6 ospf area....989
ipv6 ospf authentication....989
ipv6 ospf bfd all-neighbors....990
ipv6 ospf cost....991
ipv6 ospf dead-interval....992
ipv6 ospf encryption....992
ipv6 ospf graceful-restart helper-reject....994
ipv6 ospf hello-interval....994
ipv6 ospf priority....995
ipv6 router ospf....995
maximum-paths....996
passive-interface....996
redistribute....997
router-id....999
show crypto ipsec policy....1000
show crypto ipsec sa ipv6....1000
show ipv6 ospf database....1001
show ipv6 ospf interface....1002
show ipv6 ospf neighbor....1003

38 Policy-based Routing (PBR)....1004
description....1004
ip redirect-group....1004
ip redirect-list....1005
permit....1006
redirect....1007
seq....1009
show cam pbr....1011
show ip redirect-list....1012

39 PIM-Sparse Mode (PIM-SM)....1013
IPv4 PIM-Sparse Mode Commands....1013
clear ip pim rp-mapping....1013
clear ip pim tib....1013
debug ip pim....1014
ip pim bsr-border....1015
ip pim bsr-candidate....1015

ip pim dr-priority....1016
ip pim join-filter....1017
ip pim ingress-interface-map....1017
ip pim neighbor-filter....1018
ip pim query-interval....1018
ip pim register-filter....1019
ip pim rp-address....1019
ip pim rp-candidate....1020
ip pim sparse-mode....1021
ip pim sparse-mode sg-expiry-timer....1021
ip pim spt-threshold....1022
no ip pim snooping dr-flood....1022
show ip pim bsr-router....1023
show ip pim interface....1024
show ip pim neighbor....1025
show ip pim rp....1025
show ip pim snooping interface....1026
show ip pim snooping neighbor....1027
show ip pim snooping tib....1028
show ip pim summary....1030
show ip pim tib....1031
show running-config pim....1033
IPv6 PIM-Sparse Mode Commands....1034
ipv6 pim bsr-border....1034
ipv6 pim bsr-candidate....1034
ipv6 pim dr-priority....1035
ipv6 pim join-filter....1035
ipv6 pim query-interval....1036
ipv6 pim neighbor-filter....1036
ipv6 pim register-filter....1037
ipv6 pim rp-address....1037
ipv6 pim rp-candidate....1038
ipv6 pim sparse-mode....1039
ipv6 pim spt-threshold....1039
show ipv6 pim bsr-router....1040
show ipv6 pim interface....1040
show ipv6 pim neighbor....1041
show ipv6 pim rp....1041
show ipv6 pim tib....1042

40 Port Monitoring....1044
Description....1044

flow-based enable....1045
monitor session....1045
show config....1046
show monitor session....1047
show running-config monitor session....1047
source (port monitoring)....1048

41 Private VLAN (PVLAN)....1050
ip local-proxy-arp....1051
private-vlan mapping secondary-vlan....1052
private-vlan mode....1053
show interfaces private-vlan....1054
show vlan private-vlan....1055
show vlan private-vlan mapping....1057
switchport mode private-vlan....1058

42 Per-VLAN Spanning Tree Plus (PVST+)....1060
description....1060
disable....1060
edge-port bpdufilter default....1061
extend system-id....1061
protocol spanning-tree pvst....1062
show spanning-tree pvst....1063
spanning-tree pvst....1066
spanning-tree pvst err-disable....1067
tc-flush-standard....1068
vlan bridge-priority....1068
vlan forward-delay....1069
vlan hello-time....1070
vlan max-age....1071

43 Quality of Service (QoS)....1072
Global Configuration Commands....1072
qos-rate-adjust....1072
service-class dot1p-mapping....1073
Per-Port QoS Commands....1073
dot1p-priority....1073
rate police....1074
rate shape....1075
service-class dynamic dot1p....1076
service-class bandwidth-percentage....1077
strict-priority unicast....1077

Policy-Based QoS Commands....1078
bandwidth-percentage....1078
class-map....1079
clear qos statistics.... 1080
crypto key zeroize rsa....1081
ip ssh rekey 1081
match ip access-group.... 1082
match ip vlan....1082
match ip vrf....1083
description.... 1084
match ip dscp.... 1084
match ip precedence.... 1085
match mac access-group....1086
match mac dot1p....1087
match mac vlan.... 1087
policy-aggregate.... 1088
policy-map-input.... 1089
policy-map-output....1089
qos-policy-input....1090
qos-policy-output....1091
rate police....1091
rate shape....1092
service-policy input....1093
service-policy output.... 1094
service-queue....1094
set....1095
show qos class-map....1096
show qos policy-map....1096
show qos policy-map-input....1097
show qos policy-map-output....1098
show qos qos-policy-input....1099
show qos qos-policy-output....1099
show qos statistics....1100
show qos wred-profile....1101
test cam-usage....1102
trust....1104
wred....1105
wred ecn....1106
wred-profile....1107
dscp....1107
qos dscp-color-map....1109
qos dscp-color-policy....1110

show qos dscp-color-policy 1110
show qos dscp-color-map 1112

44 Routing Information Protocol (RIP)....1113
auto-summary.... 1113
clear ip rip....1113
debug ip rip....1114
default-information originate.... 1114
default-metric....1115
description.... 1115
distance....1116
distribute-list in.... 1117
distribute-list out....1117
ip poison-reverse....1118
ip rip receive version....1119
ip rip send version....1119
ip split-horizon....1120
maximum-paths....1120
neighbor....1121
network.... 1121
offset-list....1122
output-delay....1123
passive-interface.... 1123
redistribute....1124
redistribute ospf....1125
router rip.... 1125
show config....1126
show ip rip database.... 1126
show running-config rip.... 1127
timers basic....1128
version....1129

45 Remote Monitoring (RMON)....1130
rmon alarm....1130
rmon collection history.... 1131
rmon collection statistics....1132
rmon event.... 1133
rmon hc-alarm.... 1133
show rmon....1135
show rmon alarms....1135
show rmon events....1136
show rmon hc-alarm....1137

show rmon history........ 1138
show rmon log........ 1139
show rmon statistics........ 1140

46 Rapid Spanning Tree Protocol (RSTP)........ 1142
bridge-priority........ 1142
debug spanning-tree rstp........ 1142
description........ 1143
disable........ 1144
forward-delay........ 1144
hello-time........ 1145
max-age........ 1146
edge-port bpdufilter default........ 1146
protocol spanning-tree rstp........ 1147
show config........ 1147
spanning-tree rstp........ 1148
spanning-tree rstp........ 1149
tc-flush-standard........ 1151

47 Security........ 1152
AAA Accounting Commands........ 1152
aaa accounting........ 1152
aaa accounting suppress........ 1154
accounting........ 1154
crypto key zeroize rsa........ 1155
show accounting........ 1155
Authorization and Privilege Commands........ 1156
authorization........ 1156
aaa authorization commands........ 1157
aaa authorization role-only 1158
aaa authorization config-commands........ 1159
aaa authorization exec........ 1159
privilege level (CONFIGURATION mode)........ 1160
privilege level (LINE mode)........ 1161
Authentication and Password Commands........ 1161
aaa authentication enable........ 1161
aaa authentication login........ 1162
access-class........ 1164
enable password........ 1165
enable restricted........ 1166
enable secret........ 1166
login authentication........ 1167

password....................1168
password-attributes....................1169
service password-encryption....................1170
show privilege....................1171
show users....................1171
timeout login response....................1172
username....................1173
RADIUS Commands....................1174
debug radius....................1174
ip radius source-interface....................1175
radius-server deadtime....................1175
radius-server host....................1176
radius-server key....................1177
radius-server retransmit....................1178
radius-server timeout....................1179
role 1179
TACACS+ Commands....................1180
debug tacacs+....................1180
ip tacacs source-interface....................1181
tacacs-server host....................1181
tacacs-server key....................1182
SSH Server and SCP Commands....................1183
crypto key generate....................1183
debug ip ssh....................1184
ip scp topdir....................1185
ip ssh authentication-retries....................1185
ip ssh connection-rate-limit....................1186
ip ssh hostbased-authentication....................1186
ip ssh key-size....................1187
ip ssh password-authentication....................1187
ip ssh pub-key-file....................1188
ip ssh rekey 1189
ip ssh rhostsfile....................1189
ip ssh rsa-authentication (Config)....................1190
ip ssh rsa-authentication (EXEC)....................1191
ip ssh server....................1191
show accounting....................1194
show crypto....................1194
show ip ssh....................1195
show ip ssh client-pub-keys....................1196
show ip ssh rsa-authentication....................1197
show role 1197

show users....1198
show userroles....1199
ssh....1200
Secure DHCP Commands....1201
clear ip dhcp snooping....1201
ip dhcp relay....1201
ip dhcp snooping....1202
ip dhcp snooping database....1202
ip dhcp snooping binding....1202
ip dhcp snooping database renew....1203
ip dhcp snooping trust....1204
ip dhcp source-address-validation....1204
ip dhcp snooping vlan....1204
show ip dhcp snooping....1205
username....1205
userrole....1206

48 sFlow....1208
sflow collector....1209
sflow enable (Global)....1210
sflow enable (Interface)....1210
sflow extended-switch enable....1211
sflow polling-interval (Global)....1211
sflow polling-interval (Global)....1212
sflow sample-rate (Global)....1212
sflow sample-rate (Interface)....1213
show sflow....1214
show sflow stack-unit....1215

49 Service Provider Bridging....1216
debug protocol-tunnel....1216
protocol-tunnel....1217
protocol-tunnel destination-mac....1218
protocol-tunnel enable....1218
protocol-tunnel rate-limit....1219
show protocol-tunnel....1219

50 Simple Network Management Protocol (SNMP) and Syslog....1221
SNMP Commands....1221
clear logging auditlog....1221
show snmp....1222
show snmp engineID....1223

show snmp group....1223
show snmp user....1224
snmp ifmib ifalias long....1224
snmp-server community....1225
snmp-server contact....1226
snmp-server enable traps....1227
snmp-server engineID....1228
snmp-server group....1229
snmp-server host....1231
snmp-server location....1233
snmp-server packetsize....1234
snmp-server trap-source....1234
snmp-server user....1235
snmp-server user (for AES128-CFB Encryption)....1237
snmp-server view....1238
snmp trap link-status....1239
Syslog Commands....1240
clear logging....1240
default logging buffered....1240
default logging console....1240
logging extended....1241
default logging monitor....1242
default logging trap....1242
logging....1242
logging buffered....1243
logging console....1244
logging facility....1245
logging history....1246
logging history size....1246
logging monitor....1247
logging on....1247
logging source-interface....1248
logging synchronous....1249
logging trap....1250
logging version....1250
show logging....1251
show logging driverlog stack-unit....1252
show logging auditlog....1253
terminal monitor....1253

51 Stacking....1255
redundancy disable-auto-reboot....1255

redundancy force-failover stack-unit....1256
reset stack-unit....1256
show redundancy....1257
show system stack-ports....1258
show system stack-unit stack-group....1260
stack-unit stack-group....1260
stack-unit priority....1261
stack-unit provision....1262
stack-unit renumber....1262

52 Storm Control....1264

show storm-control broadcast....1264
show storm-control multicast....1265
show storm-control unknown-unicast....1265
storm-control broadcast (Configuration)....1266
storm-control broadcast (Interface)....1267
storm-control multicast (Configuration)....1267
storm-control multicast (Interface)....1268
storm-control unknown-unicast (Configuration)....1268
storm-control unknown-unicast (Interface)....1269

53 Spanning Tree Protocol (STP)....1270

bridge-priority....1270
debug spanning-tree....1270
description....1271
disable....1272
forward-delay....1272
hello-time....1273
max-age....1273
portfast bpdufilter default....1274
protocol spanning-tree....1274
show config....1275
show spanning-tree 0....1275
spanning-tree 0....1278

54 System Time and Date....1280

calendar set....1280
clock read-calendar....1281
clock set....1281
clock summer-time date....1282
clock summer-time recurring....1283
clock timezone....1285

clock update-calendar 1286
debug ntp 1286
ntp authenticate 1287
ntp authentication-key 1287
ntp broadcast client 1288
ntp disable 1289
ntp multicast client 1289
ntp server 1289
ntp source 1290
ntp trusted-key 1291
ntp update-calendar 1291
show calendar 1292
show clock 1292
show ntp associations 1293
show ntp status 1294

55 Tunneling 1296
tunnel-mode 1296
tunnel source 1297
tunnel keepalive 1298
tunnel allow-remote 1298
tunnel dscp 1299
tunnel destination 1300
tunnel flow-label 1301
tunnel hop-limit 1301
ip unnumbered 1302
ipv6 unnumbered 1303

56 u-Boot 1304
boot change 1304
boot selection 1304
boot show net config retries 1305
boot write net config retries 1305
boot zero 1305
default gateway 1306
enable 1306
help 1306
ignore enable password 1307
ignore startup config 1307
interface management ethernet ip address 1307
no default-gateway 1308
no interface management ethernet ip address 1308

reload..1308
show boot blc..1308
show boot selection..1309
show bootflash..1309
show bootvar..1310
show default-gateway..1311
show interface management Ethernet..1311
show interface management port config..1311
syntax help..1312

57 Uplink Failure Detection (UFD)..1313

clear ufd-disable..1313
debug uplink-state-group..1314
description..1314
downstream..1315
downstream auto-recover..1316
downstream disable links..1316
enable..1317
show running-config uplink-state-group..1318
show uplink-state-group..1318
uplink-state-group..1319
upstream..1320

58 VLAN Stacking..1322

dei enable..1322
dei honor..1323
dei mark..1323
member..1324
show interface dei-honor..1325
show interface dei-mark..1325
vlan-stack access..1326
vlan-stack compatible..1326
vlan-stack dot1p-mapping..1327
vlan-stack protocol-type..1327
vlan-stack trunk..1328

59 Virtual Link Trunking (VLT)..1331

back-up destination..1331
clear ip mroute..1332
clear ip pim tib..1332
lacp ungroup member-independent vlt..1333
multicast peer-routing timeout..1333

peer-link port-channel....1333
peer-routing....1334
peer-routing-timeout....1334
primary-priority....1335
show ip mroute....1335
show vlt backup-link....1337
show vlt brief....1338
show vlt detail....1338
show vlt inconsistency....1339
show vlt mismatch....1339
show vlt role....1340
show vlt statistics....1340
system-mac....1341
unit-id....1342
vlt domain....1343
vlt-peer-lag port-channel....1343
show vlt private-vlan....1343

60 Virtual Router Redundancy Protocol (VRRP)....1345

advertise-interval....1345
authentication-type....1346
clear counters vrrp....1346
debug vrrp....1347
description....1348
disable....1348
hold-time....1348
preempt....1349
priority....1349
show config....1350
show vrrp....1351
track....1354
virtual-address....1354
vrrp delay minimum....1355
vrrp delay reload....1356
vrrp-group....1356
VRRP for IPv6 Commands....1357
clear counters vrrp ipv6....1357
debug vrrp ipv6....1358
show vrrp ipv6....1358
vrrp-ipv6-group....1360
version 1361

61 ICMP Message Types.. 1363

62 SNMP Traps.. 1365

63 FC Flex IO Modules.. 1370

FC Flex IO Modules..1370
Data Center Bridging (DCB) for FC Flex IO Modules..1370
  Interworking of DCB Map With DCB Buffer Threshold Settings.............................1370
DCB Command... 1377
  dcb-enable..1377
DCBX Commands...1378
  advertise dcbx-appln-tlv...1378
  advertise dcbx-tlv..1378
  dcbx port-role... 1379
  dcbx version...1380
  debug dcbx.. 1380
  fcoe priority-bits...1381
  iscsi priority-bits...1382
  show interface dcbx detail..1382
ETS Commands..1385
  bandwidth-percentage..1385
  clear ets counters... 1386
  dcb-map...1386
  priority-group bandwidth pfc...1387
  scheduler..1388
  set-pgid.. 1389
  show interface ets...1390
  show qos dcb-output.. 1393
  show qos priority-groups..1394
  show stack-unit stack-ports ets details...1394
PFC Commands..1395
  clear pfc counters... 1395
  description..1396
  pfc link-delay..1396
  pfc mode on... 1397
  pfc no-drop queues... 1397
  pfc priority.. 1398
  show dcb...1399
  show interface pfc... 1399
  show interface pfc statistics..1402
  show qos dcb-input... 1403

show stack-unit stack-ports pfc details....1403
Fibre Channel over Ethernet for FC Flex IO Modules....1404
NPIV Proxy Gateway for FC Flex IO Modules....1404
dcb-map....1405
description (for FCoE maps)....1406
fabric....1406
fabric-id vlan....1407
fcf-priority....1408
fc-map....1409
fcoe priority-bits....1410
fcoe-map....1410
fka-adv-period....1411
interface vlan (NPIV proxy gateway)....1412
keepalive....1413
priority-group bandwidth pfc....1414
show fcoe-map....1415
show npiv devices....1418

64 PMUX Mode of the MXL 10/40GbE Switch I/O Module....1421
Data Center Bridging (DCB)....1421
advertise dcbx-appln-tlv....1421
advertise dcbx-tlv....1422
bandwidth-percentage....1422
dcb-enable....1423
dcb-input....1424
dcb-output....1425
dcb-policy input....1425
dcb-policy input stack-unit stack-ports all....1426
dcb-policy output....1427
dcb-policy output stack-unit stack-ports all....1428
dcb stack-unit all pfc-buffering pfc-port-count pfc-queues....1429
dcb stack-unit pfc-buffering pfc-port-count pfc-queues....1430
dcbx port-role....1430
dcbx version....1431
debug dcbx....1432
description....1433
ets mode on....1433
fcoe priority-bits....1434
iscsi priority-bits....1434
pfc link-delay....1435
pfc mode on....1435
pfc no-drop queues....1436

- pfc priority....................1437
- priority-group....................1438
- priority-group qos-policy....................1439
- priority-list....................1440
- qos-policy-output ets....................1440
- scheduler....................1441
- set-pgid....................1442
- show dcb....................1443
- show interface dcbx detail....................1443
- show interface ets....................1446
- show interface pfc....................1449
- show interface pfc statistics....................1452
- show qos dcb-input....................1453
- show qos dcb-output....................1453
- show qos priority-groups....................1454
- show stack-unit stack-ports ets details....................1454
- show stack-unit stack-ports pfc details....................1455

FIP Snooping....................1456
- clear fip-snooping database interface vlan....................1456
- feature fip-snooping....................1457
- fip-snooping enable....................1458
- fip-snooping fc-map....................1458
- fip-snooping port-mode fcf....................1459

iSCSI Optimization....................1459
- advertise dcbx-app-tlv....................1459
- iscsi aging time....................1460
- iscsi cos....................1460
- iscsi enable....................1461
- iscsi priority-bits....................1461
- iscsi profile-compellant....................1462
- iscsi target port....................1462

Interfaces....................1463
- Basic Interface Commands....................1463
- clear counters....................1463
- description....................1464
- flowcontrol....................1465
- interface....................1467
- interface ManagementEthernet....................1468
- interface range....................1469
- interface vlan....................1471
- intf-type cr4 autoneg....................1472
- keepalive....................1472

mtu.....1473
negotiation auto.....1474
portmode hybrid.....1476
stack-unit portmode.....1478
Port Channel Commands.....1479
channel-member.....1479
interface port-channel.....1480
minimum-links.....1481
Internet Group Management Protocol (IGMP).....1482
IGMP Commands.....1482
IGMP Snooping Commands.....1486
Layer 2.....1491
MAC Addressing Commands.....1491
mac-address-table aging-time.....1491
mac-address-table static.....1492
mac-address-table station-move refresh-arp.....1492
Link Aggregation Control Protocol (LACP).....1493
lacp long-timeout.....1493
lacp port-priority.....1494
port-channel mode.....1494
port-channel-protocol lacp.....1495
Link Layer Discovery Protocol (LLDP).....1496
advertise dot3-tlv.....1496
advertise management-tlv.....1496
clear lldp counters.....1497
clear lldp neighbors.....1498
debug lldp interface.....1498
disable.....1499
hello.....1500
multiplier.....1500
Quality of Service (QoS).....1501
Per-Port QoS Commands.....1501
dot1p-priority.....1501
service-class dynamic dot1p.....1502
service-class dot1p-mapping.....1503
service-class bandwidth-percentage.....1504
Policy-Based QoS Commands.....1505
bandwidth-percentage.....1505
description.....1505
policy-aggregate.....1506
policy-map-output.....1507
qos-policy-output.....1507

- service-policy output....1508
- service-queue....1508
- show qos qos-policy-output....1509

Virtual Link Trunking (VLT)....1510

- back-up destination....1510
- clear vlt statistics....1511
- lacp ungroup member-independent....1512
- peer-link port-channel....1513
- show vlt mismatch....1514
- system-mac....1515
- unit-id....1515
- vlt domain....1516
- vlt-peer-lag port-channel....1517

reload-type....1518

Uplink Failure Detection (UFD)....1520

- clear ufd-disable....1520
- debug uplink-state-group....1521
- description....1522
- downstream....1522
- downstream auto-recover....1524
- downstream disable links....1524
- enable....1525
- show running-config uplink-state-group....1526
- show uplink-state-group....1527
- uplink-state-group....1528
- upstream....1529

Simple Network Management Protocol (SNMP) and Syslog....1531

- SNMP Commands....1531
- Syslog Commands....1536

1

About this Guide

This book provides information about the Dell Networking Operating System (OS) command line interface (CLI).

This book also includes information about the protocols and features found in the Dell OS and on the Dell Networking systems supported by the Dell OS.

References

For more information about your system, refer to the following documents:

- *Dell Networking OS Configuration Guides*
- *Installation and Maintenance Guides for the MXL 10/40GbE Switch System*
- *Release Notes for the MXL 10/40GbE Switch System and Dell Networking OS version 8.3.16.4*

Objectives

This book is intended as a reference guide for the Dell OS CLI commands, with detailed syntax statements, along with usage information and sample output.

This guide contains an Appendix with a list of the request for comment (RFCs) and management information base files (MIBs) supported.

NOTE: For more information about when to use the CLI commands, refer to the *Dell Networking OS Configuration Guide* for your system.

Audience

This book is intended for system administrators who are responsible for configuring or maintaining networks. This guide assumes that you are knowledgeable in Layer 2 and Layer 3 networking technologies.

Conventions

This book uses the following conventions to describe command syntax.

`Keyword`	Keywords are in Courier font and must be entered in the CLI as listed.
parameter	Parameters are in italics and require a number or word to be entered in the CLI.
{X}	Keywords and parameters within braces must be entered in the CLI.
[X]	Keywords and parameters within brackets are optional.
x|y	Keywords and parameters separated by a bar require you to choose one option.
x||y	Keywords and parameters separated by a double bar allows you to choose any or all of the options.

Information Icons

This book uses the following information symbols:

NOTE: The Note icon signals important operational information.

CAUTION: The Caution icon signals information about situations that could result in equipment damage or loss of data.

WARNING: The Warning icon signals information about hardware handling that could result in injury.

2

CLI Basics

This chapter describes the command line interface (CLI) structure and command modes. The Dell operating software commands are in a text-based interface that allows you to use the launch commands, change command modes, and configure interfaces and protocols.

Accessing the Command Line

When the system boots successfully, you are positioned on the command line in EXEC mode and not prompted to log in. You can access the commands through a serial console port or a Telnet session. When you Telnet into the switch, you are prompted to enter a login name and password.

Example

```
telnet 172.31.1.53
Trying 172.31.1.53...
Connected to 172.31.1.53.
Escape character is '^]'.
Login: username
Password: Dell>
```

After you log in to the switch, the prompt provides you with the current command-level information. For example:

Prompt	CLI Command Mode
`Dell>`	EXEC
`Dell#`	EXEC Privilege
`Dell(conf)#`	CONFIGURATION

NOTE: For a list of all the command mode prompts, refer to the Command Modes section.

Multiple Configuration Users

When a user enters CONFIGURATION mode and another user is already in CONFIGURATION mode, the Dell Networking Operating System (OS) generates an alert warning message similar to the following:

```
Dell#conf

% Warning: The following users are currently configuring the system:

User "" on line console0
User "admin" on line vty0 ( 123.12.1.123 )
User "admin" on line vty1 ( 123.12.1.123 )
User "Irene" on line vty3 ( 123.12.1.321 )
Dell#conf
```

When another user enters CONFIGURATION mode, the Dell Networking OS sends a message similar to the following:

```
% Warning: User "admin" on line vty2 "172.16.1.210" is in configuration
```

In this case, the user is “admin” on vty2.

Navigating the CLI

The Dell Networking Operating System (OS) displays a command line interface (CLI) prompt comprised of the host name and CLI mode.

- Host name is the initial part of the prompt and is “Dell” by default. You can change the host name with the `hostname` command.
- CLI mode is the second part of the prompt and reflects the current CLI mode. For a list of the Dell Networking OS command modes, refer to the command mode list in the Accessing the Command Line section.

The CLI prompt changes as you move up and down the levels of the command structure. Starting with CONFIGURATION mode, the command prompt adds modifiers to further identify the mode. For more information about command modes, refer to the Command Modes section.

Prompt	CLI Command Mode
Dell>	EXEC
Dell#	EXEC Privilege
Dell(conf)#	CONFIGURATION
Dell(conf-if-te-0/0)# Dell(conf-if-vl-1)# Dell(conf-if-ma-0/0)# Dell(conf-if-range)#	INTERFACE
Dell(conf-line-console)# Dell(conf-line-vty)#	LINE
Dell(conf-mon-sess)#	MONITOR SESSION

Obtaining Help

As soon as you are in a command mode there are several ways to access help.

To obtain a list of keywords at any command mode:	Type a `?` at the prompt or after a keyword. There must always be a space before the `?`.

To obtain a list of keywords with a brief functional description:	Type `help` at the prompt.
To obtain a list of available options:	Type a keyword and then type a space and a `?`.
To obtain a list of partial keywords using a partial keyword:	Type a partial keyword and then type a `?`.
Example	The following is an example of typing `ip ?` at the prompt:

```
Dell(conf)#ip ?
igmp     Internet Group Management Protocol
route    Establish static routes
telnet   Specify telnet options
```

When entering commands, you can take advantage of the following timesaving features:

- The commands are not case-sensitive.
- You can enter partial (truncated) command keywords. For example, you can enter `int gig int interface` for the `interface gigabitethernet interface` command.
- To complete keywords in commands, use the TAB key.
- To display the last enabled command, use the up Arrow key.
- Use either the Backspace key or Delete key to erase the previous character.
- To navigate left or right in the Dell Networking OS command line, use the left and right Arrow keys.

The shortcut key combinations at the Dell Networking OS command line are as follows:

Key Combination	Action
CNTL-A	Moves the cursor to the beginning of the command line.
CNTL-B	Moves the cursor back one character.
CNTL-D	Deletes the character at the cursor.
CNTL-E	Moves the cursor to the end of the line.
CNTL-F	Moves the cursor forward one character.
CNTL-I	Completes a keyword.
CNTL-K	Deletes all the characters from the cursor to the end of the command line.
CNTL-L	Re-enters the previous command.
CNTL-N	Returns to the more recent commands in the history buffer after recalling commands with Ctrl-P or the up Arrow key.
CNTL-P	Recalls commands, beginning with the last command.

Key Combination	Action
CNTL-R	Re-enters the previous command.
CNTL-U	Deletes the line.
CNTL-W	Deletes the previous word.
CNTL-X	Deletes the line.
CNTL-Z	Ends continuous scrolling of the command outputs.
Esc B	Moves the cursor back one word.
Esc F	Moves the cursor forward one word.
Esc D	Deletes all the characters from the cursor to the end of the word.

Using the Keyword no Command

To disable, delete or return to default values, use the `no` form of the commands.

For most commands, if you type the keyword `no` in front of the command, you disable that command or delete it from the running configuration. In this guide, the `no` form of the command is described in the Syntax portion of the command description. For example:

Syntax

```
no {boot | default | enable | ftp-server | hardware | hostname
| ip | line | logging | monitor | service | io-aggregator
broadcast storm-control | snmp-server | username}
```

Defaults None

Command Modes CONFIGURATION

Command History

Version	Description
Version 8.3.17.0	Supported on the M I/O Aggregator.

Filtering show Commands

To find specific information, display certain information only or begin the command output at the first instance of a regular expression or phrase, you can filter the display output of a `show` command.

When you execute a `show` command, and then enter a pipe (|), one of the following parameters, and a regular expression, the resulting output either excludes or includes those parameters.

NOTE: The Dell Networking Operating System (OS) accepts a space before or after the pipe, no space before or after the pipe, or any combination. For example: `Dell#command | grep gigabit |except regular-expression | find regular-expression`.

`except`	displays only the text that does not match the pattern (or regular expression)

`find`	searches for the first occurrence of a pattern
`grep`	displays text that matches a pattern.
`no-more`	does not paginate the display output
`save`	copies the output to a file for future use

The grep command option has an ignore-case sub-option that makes the search case-insensitive. For example, the commands:

Displaying All Output

To display the output all at once (not one screen at a time), use the `no-more` option after the pipe. This operation is similar to the `terminal length screen-length` command except that the `no-more` option affects the output of just the specified command. For example: `Dell#show running-config| no-more`.

Filtering the Command Output Multiple Times

You can filter a single command output multiple times. To filter a command output multiple times, place the `save` option as the last filter. For example: `Dell# command | grep regular-expression | except regular-expression | grep other-regular-expression | find regular-expression | no-more | save`.

Command Modes

To navigate and launch various CLI modes, use specific commands. Navigation to these modes is described in the following sections.

EXEC Mode

When you initially log in to the switch, by default, you are logged in to EXEC mode. This mode allows you to view settings and enter EXEC Privilege mode, which is used to configure the device.

When you are in EXEC mode, the > prompt is displayed following the host name prompt, which is “Dell” by default. You can change the host name prompt using the `hostname` command.

NOTE: Each mode prompt is preceded by the host name.

EXEC Privilege Mode

The `enable` command accesses EXEC Privilege mode. If an administrator has configured an “Enable” password, you are prompted to enter it.

EXEC Privilege mode allows you to access all the commands accessible in EXEC mode, plus other commands, such as to clear address resolution protocol (ARP) entries and IP addresses. In addition, you can access CONFIGURATION mode to configure interfaces, routes and protocols on the switch. While you are logged in to EXEC Privilege mode, the # prompt displays.

CONFIGURATION Mode

In EXEC Privilege mode, use the `configure` command to enter CONFIGURATION mode and configure routing protocols and access interfaces.

To enter CONFIGURATION mode:

1. Verify that you are logged in to EXEC Privilege mode.
2. Enter the `configure` command. The prompt changes to include (conf).

From this mode, you can enter INTERFACE mode by using the `interface` command.

INTERFACE Mode

Use INTERFACE mode to configure interfaces or IP services on those interfaces. An interface can be physical (for example, a Gigabit Ethernet port) or virtual (for example, the Null interface).

To enter INTERFACE mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `interface` command and then enter an interface type and interface number that is available on the switch.

The prompt changes to include the designated interface and slot/port number. For example:

Prompt	Interface Type
`Dell(conf-if)#`	INTERFACE mode
`Dell(conf-if-te-0/0)#`	Ten-Gigabit Ethernet interface then slot/port information
`Dell(conf-if-fo-0/0)#`	Forty-Gigabit Ethernet interface then slot/port information
`Dell(conf-if-lo-0)#`	Loopback interface number
`Dell(conf-if-nu-0)#`	Null Interface then zero
`Dell(conf-if-po-0)#`	Port-channel interface number
`Dell(conf-if-vl-0)#`	VLAN Interface then VLAN number (range 1–4094)
`Dell(conf-if-ma-0/0)#`	Management Ethernet interface then slot/port information
`Dell(conf-if-range)#`	Designated interface range (used for bulk configuration).

IP ACCESS LIST Mode

To enter IP ACCESS LIST mode and configure either standard or extended access control lists (ACLs), use the `ip access-list standard` or `ip access-list extended` command.

To enter IP ACCESS LIST mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Use the `ip access-list standard` or `ip access-list extended` command. Include a name for the ACL. The prompt changes to include (`conf-std-nacl`) or (`conf-ext-nacl`).

You can return to CONFIGURATION mode by using the `exit` command.

LINE Mode

To configure the console or virtual terminal parameters, use LINE mode.

To enter LINE mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `line` command. Include the keywords `console` or `vty` and their line number available on the switch. The prompt changes to include (`config-line-console`) or (`config-line-vty`).

You can exit this mode by using the `exit` command.

MAC ACCESS LIST Mode

To enter MAC ACCESS LIST mode and configure either standard or extended access control lists (ACLs), use the `mac access-list standard` or `mac access-list extended` command.

To enter MAC ACCESS LIST mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Use the `mac access-list standard` or `mac access-list extended` command. Include a name for the ACL. The prompt changes to include (`conf-std-macl`) or (`conf-ext-macl`).

You can return to CONFIGURATION mode by using the `exit` command.

MULTIPLE SPANNING TREE Mode

To enable and configure the multiple spanning tree protocol (MSTP), use MULTIPLE SPANNING TREE mode , as described in Multiple Spanning Tree Protocol (MSTP).

To enter MULTIPLE SPANNING TREE mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `protocol spanning-tree mstp` command.

You can return to CONFIGURATION mode by using the `exit` command.

Per-VLAN SPANNING TREE (PVST+) Plus Mode

To enable and configure the Per-VLAN Spanning Tree (PVST+) protocol, use PVST+ mode. For more information, refer to Per-VLAN Spanning Tree Plus (PVST+).

NOTE: The protocol name is PVST+, but the plus sign is dropped at the CLI prompt.

To enter PVST+ mode:

1. Verify that you are logged in to CONFIGURATION mode.

2. Enter the `protocol spanning-tree pvst` command. The prompt changes to include (`conf-pvst`).

You can return to CONFIGURATION mode by using the `exit` command.

PREFIX-LIST Mode

To configure a prefix list, use PREFIX-LIST mode.

To enter PREFIX-LIST mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `ip prefix-list` command. Include a name for the prefix list. The prompt changes to include (`conf-nprefixl`).

You can return to CONFIGURATION mode by using the `exit` command.

PROTOCOL GVRP Mode

To enable and configure GARP VLAN Registration Protocol (GVRP), use PROTOCOL GVRP mode. For more information, refer to GARP VLAN Registration (GVRP).

To enter PROTOCOL GVRP mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `protocol gvrp` command. The prompt changes to include (`config-gvrp`).

You can return to CONFIGURATION mode by using the `exit` command.

RAPID SPANNING TREE (RSTP) Mode

To enable and configure RSTP, use RSTP mode. For more information, refer to Rapid Spanning Tree Protocol (RSTP).

To enter RSTP mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `protocol spanning-tree rstp` command. The prompt changes to include (`conf-rstp`).

You can return to CONFIGURATION mode by using the `exit` command.

ROUTE-MAP Mode

To configure a route map, use ROUTE-MAP mode.

To enter ROUTE-MAP mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Use the `route-map` *`map-name`* `[permit | deny]` `[`*`sequence-number`*`]` command. The prompt changes to include (`config-route-map`).

You can return to CONFIGURATION mode by using the `exit` command.

ROUTER OSPF Mode

To configure OSPF, use ROUTER OSPF mode. For more information, refer to Open Shortest Path First (OSPF).

To enter ROUTER OSPF mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `router ospf {process-id}` command. The prompt changes to include (`conf-router_ospf-id`).

You can switch to INTERFACE mode by using the `interface` command or you can switch to ROUTER RIP mode by using the `router rip` command.

ROUTER RIP Mode

To enable and configure Router Information Protocol (RIP), use ROUTER RIP mode. For more information, refer to Routing Information Protocol (RIP).

To enter ROUTER RIP mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `router rip` command. The prompt changes to include (`conf-router_rip`).

You can return to CONFIGURATION mode by using the `exit` command.

SPANNING TREE Mode

To enable and configure the Spanning Tree protocol, use SPANNING TREE mode. For more information, refer to Spanning Tree Protocol (STP).
To enter SPANNING TREE mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `protocol spanning-tree` *stp-id* command. The prompt changes to include (`conf-stp`).

You can return to CONFIGURATION mode by using the `exit` command.

3

File Management

This chapter contains command line interface (CLI) commands needed to manage the configuration files as well as other file management commands.

The commands in this chapter are supported by the Dell Networking Operating System (OS).

cd

Change to a different working directory.

Syntax	`cd directory`
Parameters	*directory* — (OPTONAL) Enter the following: • `flash:` (internal Flash) or any sub-directory • `usbflash:` (external Flash) or any sub-directory
Command Modes	EXEC Privilege
Command History	Version 8.3.16.0 — Introduced on the MXL 10/40GbE Switch IO Module.

copy

Copy one file to another location. The Dell Networking Operating System (OS) supports IPv4 addressing for FTP, TFTP, and SCP (in the *hostip* field).

Syntax	`copy source-file-url destination-file-url`
Parameters	Enter the following location keywords and information:

file-url	To copy a file from the internal FLASH	Enter the keyword `flash://` then the filename.

To copy the running configuration	Enter the keywords `running-config`.
To copy the startup configuration	Enter the keywords `startup-config`.
To copy a file on the external FLASH	Enter the keyword `slot0://` then the filename.

Command Modes

EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The Dell Networking OS supports a maximum of 100 files at the root directory level, on both the internal and external Flash.

The `usbflash` commands are supported. For a list of approved USB vendors, refer to the *Dell Networking OS Release Notes*.

When copying a file to a remote location (for example, using Secure Copy [SCP]), enter only the keywords and Dell Networking OS prompts you need for the rest of the information. For example, when using SCP, you can enter `copy running-config scp:` where `running-config` is the source and the target is specified in the ensuing prompts. The Dell Networking OS prompts you to enter any required information, as needed for the named destination—remote destination, destination filename, user ID, password, and so forth.

When you use the `copy running-config startup-config` command to copy the running configuration (the startup configuration file amended by any configuration changes made since the system was started) to the startup configuration file, the Dell Networking OS creates a backup file on the internal flash of the startup configuration.

The Dell Networking OS supports copying the running-configuration to a TFTP server or to an FTP server. For example:

- `copy running-config tftp:`
- `copy running-config ftp:`

Example

```
Dell#copy running-config scp:
Address or name of remote host []: 10.10.10.1
Port number of the server [22]: 99
Destination file name [startup-config]: old_running
User name to login remote host: sburgess
Password to login remote host:

Password to login remote host? dilling
```

In this `copy scp: flash:` example, specifying `SCP` in the first position indicates that the target is to be specified in the ensuing prompts. Entering `flash:` in the second position indicates that the target is the internal Flash. The source is on a secure server running SSH, so you are prompted for the user datagram protocol (UDP) port of the SSH server on the remote host.

Example

```
Dell#copy scp: flash:
Address or name of remote host []: 10.11.199.134
Port number of the server [22]: 99
Source file name []: test.cfg
User name to login remote host: admin
Password to login remote host:
Destination file name [test.cfg]: test1.cfg
```

Related Commands

cd – changes the working directory.

copy running-config startup-config

Copy running configuration to the startup configuration.

Syntax

`copy running-config startup-config {duplicate}`

Command Modes

EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

This command is useful for quickly making a changed configuration on one chassis available on external flash in order to move it to another chassis.

delete

Delete a file from the flash. After deletion, files cannot be restored.

Syntax

`delete flash: ([flash://]filepath) usbflash ([usbflash://]filepath)`

Parameters

flash-url	Enter the following location and keywords: • For a file or directory on the internal Flash, enter `flash://` then the filename or directory name. • For a file or directory on an external USB drive, enter `usbflash://` then the filename or directory name.
no-confirm	(OPTIONAL) Enter the keywords `no-confirm` to specify that the Dell Networking OS does not require user input for each file prior to deletion.

Command Modes

EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#dir
Directory of flash:

1  drwx  4096      Jan 01 1980 00:00:00 +00:00 .
2  drwx  2048      Mar 06 2010 00:36:21 +00:00 ..
3  drwx  4096      Feb 25 2010 23:32:50 +00:00 TRACE_LOG_DIR
4  drwx  4096      Feb 25 2010 23:32:50 +00:00 CORE_DUMP_DIR
5  d---  4096      Feb 25 2010 23:32:50 +00:00 ADMIN_DIR
6  -rwx  720969768 Mar 05 2010 03:25:40 +00:00 6gb
7  -rwx  4260      Mar 03 2010 22:04:50 +00:00 prem-23-5-12
8  -rwx  31969685  Mar 05 2010 17:56:26 +00:00
DellS-XL-8-3-16-148.bin
9  -rwx  3951      Mar 06 2010 00:36:18 +00:00 startup-config

flash: 2143281152 bytes total (1389801472 bytes free)
Dell#
```

Related Commands

cd — Changes the working directory.

format flash

Erase all existing files and reformat the filesystem in the internal flash memory. After the filesystem is formatted, files cannot be restored.

Syntax

`format {flash: | usbflash:}`

Defaults

flash memory

Command Modes

EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

You must include the colon (:) when entering this command.

CAUTION: This command deletes all files, including the startup configuration file. So, after executing this command, consider saving the running config as the startup config (use the `write memory` command or `copy run start` command).

Related Commands

copy — copies the current configuration to either the startup-configuration file or the terminal.

show file — displays the contents of a text file in the local filesystem.

show file-systems — displays information about the file systems on the system.

HTTP Copy via CLI

Copy one file to another location. Dell Networking OS supports IPv4 and IPv6 addressing for FTP, TFTP, and SCP (in the *hostip* field).

This feature is supported on S6000 Z9000 S4810 S4820T platform.

Syntax

```
copy http://10.16.206.77/sample_file flash://sample_filecopy
flash://sample_file http://10.16.206.77/sample_file
```

You can copy from the server to the switch and vice-versa.

Parameters

`copy http: flash:`	Address or name of remote host []: 10.16.206.77 Port number of the server [80]: Source file name []: sample_file User name to login remote host: x Password to login remote host: Destination file name [sample_file]:

Defaults
None.

Command Modes
EXEC

Command History

Version 9.3(0.1)	Introduced on the S6000, Z9000, S4810, and S4820T.

Example

```
copy http://admin:admin123@10.16.206.77/sample_file flash://
sample_file
```

Related Commands

`copy ftp:flash`

Copy files from FTP server to switch

logging coredump

Enable coredump.

Syntax

```
logging coredump stack-unit all
```

Command Modes CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The kernel coredump can be large and may take five to 30 minutes to upload.

The Dell Networking OS does not overwrite application coredumps so you should delete them as necessary to conserve space on the flash; if the flash is out of memory, the coredump is aborted.

If the FTP server is not reachable, the application coredump is aborted. The Dell Networking OS completes the coredump process and waits until the upload is complete before rebooting the system.

Related Commands logging coredump server — designates a server to upload kernel coredumps.

logging coredump server

Designate a server to upload core dumps.

Syntax

```
logging coredump server {ipv4-address} username name password
[type] password
```

Parameters

{ipv4-address }	Enter the server IPv4 address (A.B.C.D).
name	Enter a username to access the target server.
type	Enter the password type: • Enter `0` to enter an unencrypted password. • Enter `7` to enter a password that has already been encrypted using a Type 7 hashing algorithm.
password	Enter a password to access the target server.

Defaults Crash kernel files are uploaded to flash by default.

Command Modes CONFIGURATION

Command History

Version 8.4.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Because flash space may be limited, using this command ensures your entire crash kernel files are uploaded successfully and completely. Only a single coredump server can be configured. Configuration of a new coredump server over-writes any previously configured server.

NOTE: You must disable `logging coredump` before you designate a new server destination for your core dumps.

Related Commands	logging coredump – disables the kernel coredump

pwd

Display the current working directory.

Syntax	`pwd`
Command Modes	EXEC Privilege
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#pwd
flash:
Dell#
```

Related Commands	cd – changes the directory.

rename

Rename a file in the local file system.

Syntax `rename` *`url url`*

Parameters

url Enter the following keywords and a filename:

- For a file on the internal Flash, enter `flash://` then the filename.
- For a file on an external USB drive, enter `usbflash://` then the filename.

Command Modes	EXEC Privilege
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

show boot system

Displays information about boot images currently configured on the system.

Syntax	`show boot system stack-unit {0-5 | all}`

Parameters

0–5	Enter this information to display the boot image information of only the entered stack-unit.
all	Enter the keyword `all` to display the boot image information of all the stack-units in the stack.

Defaults: none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show boot system stack-unit all
Current system image information in the system:
=============================================
Type      Boot Type         A             B
---------------------------------------------
Stack-unit 0 is not present.
Stack-unit 1 is not present.
Stack-unit 2 is not present.
Stack-unit 3 is not present.
Stack-unit 4 is not present.
Stack-unit 5 DOWNLOAD BOOT 9-1-0-675    9-1-0-684
```

show file

Display contents of a text file in the local filesystem.

Syntax	`show file url`

Parameters

url — Enter one of the following:

- For a file on the internal Flash, enter `flash://` then the filename.
- For a file on the external Flash, enter `usbflash://` then the filename.

Command Modes: EXEC Privilege

Command History	
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show file flash://startup-config
! Version E8-3-16-29
! Last configuration change at Thu Apr 26 19:19:02 2012 by
default
! Startup-config last updated at Thu Apr 26 19:19:04 2012 by
default
!
boot system stack-unit 0 primary system: A:
boot system stack-unit 0 secondary tftp://10.11.200.241/dt-
m1000e-5-c2
boot system gateway 10.11.209.254
!
redundancy auto-synchronize full
redundancy disable-auto-reboot stack-unit
!
redundancy disable-auto-reboot stack-unit 0
redundancy disable-auto-reboot stack-unit 1
redundancy disable-auto-reboot stack-unit 2
redundancy disable-auto-reboot stack-unit 3
redundancy disable-auto-reboot stack-unit 4
redundancy disable-auto-reboot stack-unit 5
!
service timestamps log datetime
logging coredump stack-unit all
!
hostname FTOS
--More--
```

Related Commands

format flash — Erases all the existing files and reformats the filesystem in the internal flash memory.

show file-systems — displays information about the file systems on the system.

show file-systems

Display information about the file systems on the system.

Syntax

```
show file-systems
```

Command Modes

EXEC Privilege

Command History	
Version 8.3.16.0	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show file-systems
Size(b)       Free(b)     Feature Type       Flags Prefixes
 2143281152   2000936960  FAT32   USERFLASH  rw    flash:
15848660992    831594496  FAT32   USBFLASH   rw    usbflash:
          -            -       -  network    rw    ftp:
          -            -       -  network    rw    tftp:
                -              -       -    network     rw     scp:
Dell#
```

Command Fields

Field	Description
size(b)	Lists the size (in bytes) of the storage location. If the location is remote, no size is listed.
Free(b)	Lists the available size (in bytes) of the storage location. If the location is remote, no size is listed.
Feature	Displays the formatted DOS version of the device.
Type	Displays the type of storage. If the location is remote, the word `network` is listed.
Flags	Displays the access available to the storage location. The following letters indicate the level of access: • r = read access • w = write access
Prefixes	Displays the name of the storage location.

Related Commands

format flash — Erases all the existing files and reformats the filesystem in the internal flash memory.

show file — Displays the contents of a text file in the local filesystem.

show startup-config — Displays the current SFM status.

show os-version

Display the release and software image version information of the image file specified.

Syntax `show os-version [file-url]`

Parameters

file-url	(OPTIONAL) Enter the following location keywords and information: • For a file on the internal Flash, enter `flash://` then the filename. • For a file on an FTP server, enter `ftp://user:password@hostip/filepath`. • For a file on a TFTP server, enter `tftp://hostip/filepath`. • For a file on the external Flash, enter `usbflash://filepath` then the filename.

Defaults none

Command Modes EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

NOTE: A filepath that contains a dot (.) is not supported.

Example

```
Dell#show os-version

RELEASE IMAGE INFORMATION :
--------------------------------------------------------
   Platform    Version    Size        ReleaseTime
IOM-Series: XL 9-1-0-848  31962011 Mar 20 2012 09:26:46

TARGET IMAGE INFORMATION :
--------------------------------------------------------
   Type  Version    Target          checksum
runtime  9-1-0-848  Control  Processor passed

BOOT IMAGE INFORMATION :
--------------------------------------------------------
      Type  Version   Target           checksum
boot flash  4.0.1.0bt Control   Processor passed

BOOTSEL IMAGE INFORMATION :
--------------------------------------------------------
         Type  Version     Target        checksum
boot selector  4.0.0.0bt  Control  Processor passed

CPLD IMAGE INFORMATION :
-------------------------------------------------------
       Card    CPLD Name       Version
Stack-unit 5  IOM SYSTEM CPLD        5
Dell#
```

show running-config

Display the current configuration and display changes from the default values.

Syntax `show running-config [`*`entity`*`] [configured] [status]`

Parameters

entity (OPTIONAL) To display that entity's current (non-default) configuration, enter one of the following keywords:

NOTE: If you did not configure anything that entity, nothing displays and the prompt returns.

aaa	for the current AAA configuration
acl	for the current ACL configuration

arp	for the current static ARP configuration
boot	for the current boot configuration
class-map	for the current class-map configuration
fefd	for the current FEFD configuration
ftp	for the current FTP configuration
fvrp	for the current FVRP configuration
host	for the current host configuration
hardware-monitor	for hardware-monitor action-on-error settings
igmp	for the current IGMP configuration
interface	for the current interface configuration
line	for the current line configuration
load-balance	for the current port-channel load-balance configuration
logging	for the current logging configuration
mac	for the current MAC ACL configuration
mac-address-table	for the current MAC configuration
management-route	for the current Management port forwarding configuration
mroute	for the current Mroutes configuration
ntp	for the current NTP configuration
ospf	for the current OSPF configuration
pim	for the current PIM configuration
policy-map-input	for the current input policy map configuration
policy-map-output	for the current output policy map configuration
prefix-list	for the current prefix-list configuration
privilege	for the current privilege configuration
radius	for the current RADIUS configuration
resolve	for the current DNS configuration
rip	for the current RIP configuration

route-map	for the current route map configuration
snmp	for the current SNMP configuration
spanning-tree	for the current spanning tree configuration
static	for the current static route configuration
status	for the file status information
tacacs+	for the current TACACS+ configuration
tftp	for the current TFTP configuration
users	for the current users configuration
wred-profile	for the current wred-profile configuration

configured	(OPTIONAL) Enter the keyword `configuration` to display line card interfaces with non-default configurations only.
status	(OPTIONAL) Enter the keyword `status` to display the checksum for the running configuration and the start-up configuration.

Command Modes

EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show running-config
Current Configuration ...
! Version E8-3-16-29
! Last configuration change at Thu Apr 26 19:19:21 2012 by
admin
! Startup-config last updated at Thu Apr 26 19:19:04 2012 by
default
!
boot system stack-unit 0 primary system: A:
boot system stack-unit 0 secondary tftp://10.11.200.241/dt-
m1000e-5-c2
boot system gateway 10.11.209.254
!
redundancy auto-synchronize full
redundancy disable-auto-reboot stack-unit
!
redundancy disable-auto-reboot stack-unit 0
redundancy disable-auto-reboot stack-unit 1
redundancy disable-auto-reboot stack-unit 2
redundancy disable-auto-reboot stack-unit 5
!--More--
service timestamps log datetime
logging coredump stack-unit all
!
hostname FTOS
```

```
!
...
```

Example

```
Dell#show running-config status

running-config bytes 4306, checksum 0x4D55EE70
startup-config bytes 4344, checksum 0x6472C5E
Dell#
```

Usage Information

The `status` option allows you to display the size and checksum of the running configuration and the startup configuration.

show startup-config

Display the startup configuration.

Syntax

```
show startup-config
```

Command Modes

EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show startup-config
! Version E8-3-16-29
! Last configuration change at Thu Apr 26 19:19:02 2012 by
default
! Startup-config last updated at Thu Apr 26 19:19:04 2012 by
default
!
boot system stack-unit 0 primary system: A:
boot system stack-unit 0 secondary tftp://10.11.200.241/
dt-m1000e-5-c2
boot system gateway 10.11.209.254
!
redundancy auto-synchronize full
redundancy disable-auto-reboot stack-unit
!
redundancy disable-auto-reboot stack-unit 0
redundancy disable-auto-reboot stack-unit 1
redundancy disable-auto-reboot stack-unit 2
redundancy disable-auto-reboot stack-unit 3
--More--
```

Related Commands

show running-config — displays the current (running) configuration.

show version

Display the current Dell Networking OS version information on the system.

Syntax	`show version`
Command Modes	EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show version
Dell Force10 Real Time Operating System Software
Dell Force10 Operating System Version: 1.0
Dell Force10 Application Software Version: E8-3-16-29
Copyright (c) 1999-2012 by Dell Inc. All Rights Reserved.
Build Time: Thu Apr 26 05:41:48 PDT 2012
Build Path: /sites/sjc/work/build/buildSpaces/build03/
E8-3-16/SW/SRC/Cp_src/
Tacacs
FTOS uptime is 13 hour(s), 29 minute(s)

System image file is "system://A"

System Type: MXL-10/40GbE
Control Processor: MIPS RMI XLP with 2147483648 bytes of
memory.

256M bytes of boot flash memory.

  1 34-port GE/TE/FG (XL)
 48 Ten GigabitEthernet/IEEE 802.3 interface(s)
  2 Forty GigabitEthernet/IEEE 802.3 interface(s)
```

Command Fields

Lines Beginning With	Description
Dell Force10 Network...	Name of the operating system
Dell Force10 Operating...	OS version number
Dell Force10 Application...	Software version
Copyright (c)...	Copyright information
Build Time...	Software build’s date stamp
Build Path...	Location of the software build files loaded on the system
Dell Force10 uptime is...	Amount of time the system has been up
System image...	Image file name

Lines Beginning With	Description
Chassis Type:	Chassis type (for example, E1200, E600, E600i, E300, C300, C150, S25, S50, S55, S60, S4810)
Control Processor:...	Control processor information and amount of memory on processor
128K bytes...	Amount and type of memory on system
1 34 Port	Hardware configuration of the system, including the number and type of physical interfaces available

upgrade boot

Upgrade the bootflash image or bootselector image.

Syntax

```
upgrade boot {all | bootflash-image | bootselector-image}
stack-unit {0-5 | all} {booted | flash: |ftp: | tftp: |
usbflash:} (A: | B:}
```

Parameters

all	Enter the keyword `all` to change both the bootflash and bootselecter images.
bootflash-image	Enter the keywords `bootflash-image` to change the bootflash image.
bootselector-image	Enter the keywords `bootselector-image` to change the bootselector image.
0–5	Enter the keyword `0-5` to upgrade all stack-units.
all	Enter the keyword `all` to upgrade all the member stack-units.
booted	Enter the keyword `booted` to upgrade from the current image in the MXL 10/40GbE Switch.
ftp:	After entering the keyword `ftp:`, you can either follow it with the location of the source file in this form: `//userid:password@hostip/filepath` or press Enter to launch a prompt sequence.
tftp:	After entering the keyword `tftp:`, you can either follow it with the location of the source file in this form: `//hostlocation/filepath` or press Enter to launch a prompt sequence.
flash:	After entering the keyword `flash:`, you can either follow it with the location of the source file in this form: `//filepath` or press Enter to launch a prompt sequence.

usbflash:	After entering the keyword `usbflash:`, you can either follow it with the location of the source file in this form: `//filepath` or press Enter to launch a prompt sequence.
A:	Enter this keyword to upgrade the bootflash partition A.
B:	Enter this keyword to upgrade the bootflash partition B.

Defaults

none

Command Modes

EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

You must reload the Dell Networking OS after executing this command.

Example

```
Dell#upgrade boot ?
all                 Upgrade both boot flash image and selector
image
bootflash-image     Upgrade boot flash image
bootselector-image  Upgrade boot selector image
Dell#
```

upgrade system

Upgrade the bootflash image or system image.

Syntax

`upgrade system {flash: | ftp: | scp: | tftp: | usbflash: | stack-unit {0-5 | all} {A: | B:}`

Parameters

0–5	Enter the keyword `0–5` to upgrade only the mentioned stack-unit.
all	Enter the keyword `all` to upgrade all the member units of the stack.
ftp	After entering the keyword `ftp` you can either follow it with the location of the source file in this form:`//userid:password@hostip/filepath`, or press Enter to launch a prompt sequence.
scp	After entering the keyword `scp` you can either follow it with the location of the source file in this form:`//userid:password@hostip/filepath`, or press Enter to launch a prompt sequence.
tftp	After entering the keyword `tftp` you can either follow it with the location of the source file in this form:`//filepath`, or press Enter to launch a prompt sequence.

flash	After entering the keyword `flash` you can either follow it with the location of the source file in this form:`//filepath`, or press Enter to launch a prompt sequence.
usbflash	After entering the keyword `usbflash` you can either follow it with the location of the source file in this form:`//filepath`, or press Enter to launch a prompt sequence.
A:	Enter this keyword to upgrade the bootflash partition A.
B:	Enter this keyword to upgrade the bootflash partition B.

Defaults

none

Command Modes

EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Reset the card using the `power-cycle` option after restoring the FPGA command.

Example

```
Dell#upgrade system ?
flash:         Copy from flash file system (flash://filepath)
ftp:           Copy from remote file system, IPv4 or IPv6,
(ftp:/
/userid:password@hostip/filepath)
scp:           Copy from remote file system, IPv4 or IPv6,
(scp:/
/userid:password@hostip/filepath)
stack-unit Sync image to the stack-unit
tftp:          Copy from remote file system, IPv4 or IPv6,
(tftp:/
/hostip/filepath)
usbflash:      Copy from usbflash file system (usbflash://
filepath)
Dell#
```

verify

Validate the software image on the flash drive after the image has been transferred to the system, but before the image has been installed.

Syntax

`verify { md5 | sha256 }[ flash:// ] img-file [hash-value]`

Parameters

md5	Enter the `md5` keyword to use the MD5 message-digest algorithm.
sha256	Enter the `sha256` keyword to use the SHA256 Secure Hash Algorithm

flash://	(Optional). Enter the `flash://` keyword. The default is to use the flash drive. You can just enter the image file name.
img-file	Enter the name the Dell Networking software image file to validate.
hash-value	(Optional). Enter the relevant hash published on i-Support.

Defaults	flash drive
Command Modes	EXEC mode
Command History	Version 9.5.(0.0) Introduced on the Z9000, S6000, S4820T, S4810, MXL

Usage Information

You can enter this command in the following ways:

- **verify md5 flash**://*img-file*
- **verify md5 flash**://*img-file <hash-value>*
- **verify sha256 flash**://*img-file*
- **verify sha256 flash**://*img-file <hash-value>*

Example

Without Entering the Hash Value for Verification using SHA256

```
Dell# verify sha256 flash://FTOS-SE-9.5.0.0.bin
SHA256 hash for FTOS-SE-9.5.0.0.bin:
e6328c06faf814e6899ceead219afbf9360e986d692988023b749e6b2093e93
3
```

Entering the Hash Value for Verification using SHA256

```
Dell# verify sha256 flash://FTOS-SE-9.5.0.0.bin
e6328c06faf814e6899ceead219afbf9360e986d692988023b749e6b2093e93
3
SHA256 hash VERIFIED for FTOS-SE-9.5.0.0.bin
```

4

Control and Monitoring

This chapter describes control and monitoring for the MXL 10/40GbE Switch IO Module.

asset-tag

Assign and store a unique asset-tag to the stack member.

Syntax

`asset-tag stack-unit unit id Asset-tag ID`

To remove the asset tag, use `no stack-unit unit-id Asset-tag ID` command.

Parameters

stack-unit *unit-id*	Enter the keywords`stack-unit` then the `unit-id` to assign a tag to the specific member. The range is from 0 to 5.
Asset-tag ID	Enter a unique asset-tag ID to assign to the stack member. This option accepts a maximum of 10 characters, including all special characters except double quotes. To include a space in the asset-tag, enter a space within double quotes.

Defaults

No asset-tag is assigned.

Command Modes

EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

show system — Displays the current status of all stack members or a specific member.

asf-mode

Enable alternate store and forward (ASF) mode and forward packets as soon as a threshold is reached.

Syntax

`asf-mode stack-unit {unit-id | all} queue size`

To return to standard Store and Forward mode, use the `no asf-mode stack unit` command.

Parameters

unit-id	Enter the stack member unit identifier of the stack member to reset. The range is from 0 to 5 or `all`.
queue size	Enter the queue size of the stack member. The range is from 0 to 5.

Defaults
Not configured

Command Modes
CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information
You *must* save the configuration and reload the system to implement ASF. When you enter the command, the system sends a message stating that the new mode is enabled when the system reloads.

banner exec

Configure a message that is displayed when your enter EXEC mode.

Syntax
`banner exec c line c`

Parameters

c	Enter the keywords `banner exec`, then enter a character delineator, represented here by the letter *c*. Press ENTER.
line	Enter a text string for your banner message ending the message with your delineator. In the following example, the delineator is a percent character (%); the banner message is “testing, testing”.

Defaults
No banner is displayed.

Command Modes
CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information
Optionally, use the `banner exec` command to create a text string that displays when you accesses EXEC mode. The `exec-banner` command toggles that display.

Example

```
Dell(conf)#banner exec ?
LINE         c banner-text(max length 255) c, where 'c' is a
delimiting
character

Dell(conf)#banner exec %
Enter TEXT message. End with the character '%'.
This is the banner%
Dell(conf)#end
Dell#exit
```

```
4d21h5m: %STKUNIT0-M P:CP %SEC-5-LOGOUT: Exec session is
terminated for user on
line console

This is the banner

Dell Force10 con0 now available

Press RETURN to get started.

This is the banner
```

Related Commands

banner login — sets a banner for login connections to the system.

banner motd — sets a Message of the Day banner.

exec-banner — Enables the display of a text string when you enter EXEC mode.

line — enables and configures the console and virtual terminal lines to the system.

banner login

Set a banner to display when logging on to the system.

Syntax

`banner login {keyboard-interactive | no keyboard-interactive} [c *line* c]`

Parameters

keyboard-interactive	Enter the keyword `keyboard-interactive` to require a carriage return (CR) to get the message banner prompt.
c	Enter a delineator character to specify the limits of the text banner. The delineator is a percent character (%).
line	Enter a text string for your text banner message ending the message with your delineator. The delineator is a percent character (%). Range: maximum of 50 lines, up to 255 characters per line

Defaults

No banner is configured and the CR is required when creating a banner.

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

A login banner message displays only in EXEC Privilege mode after entering the `enable` command then the password. These banners do not display to users in EXEC mode.

Example

```
Dell(conf)#banner login ?
keyboard-interactive Press enter key to get prompt
LINE                 c banner-text(max length 255) c, where
```

```
'c' is a delimiting
character
Dell(conf)#no banner login ?
keyboard-interactive  Prompt will be displayed by default
<cr>
Dell(conf)#banner login keyboard-interactive

Enter TEXT message. End with the character '%'.
This is the banner%
Dell(conf)#end
Dell#exit

13d21h9m: %STKUNIT0-M:CP %SEC-5-LOGOUT: Exec session is
terminated for user on
line console
This is the banner
Dell Force10 con0 now available
Press RETURN to get started.
13d21h10m: STKUNIT0-M:CP %SEC-5-LOGIN_SUCCESS: Login
successful for user on line
console
This is the banner
```

Related Commands	banner motd — sets a Message of the Day banner. exec-banner — enables the display of a text string when you enter EXEC mode.

banner motd

Set a message of the day (MOTD) banner.

Syntax `banner motd c line c`

Parameters

c	Enter a delineator character to specify the limits of the text banner. The delineator is a percent character (%).
line	Enter a text string for your message of the day banner message ending the message with your delineator. The delineator is a percent character (%).

Defaults No banner is configured.

Command Modes CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information A MOTD banner message displays only in EXEC Privilege mode after entering the `enable` command then the password. These banners do not display to users in EXEC (non-privilege) mode.

Related Commands	banner exec — enables the display of a text string when you enter EXEC mode. banner login — sets a banner to display after successful login to the system.

clear alarms

Clear alarms on the system.

Syntax	`clear alarms`
Command Modes	EXEC Privilege
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	This command clears alarms that are no longer active. If an alarm situation is still active, it is seen in the system output.

clear command history

Clear the command history log.

Syntax	`clear command history`
Command Modes	EXEC Privilege
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	show command-history — displays a buffered log of all the commands all users enter along with a time stamp.

clear line

Reset a terminal line.

Syntax	`clear line {line-number	console 0	vty number}`
Parameters	

line-number	Enter a number for one of the 12 terminal lines on the system. The range is from 0 to 11.
console 0	Enter the keywords `console 0` to reset the console port.

vty number	Enter the keyword `vty` then a number to clear a terminal line. The range is from 0 to 9.

Command Modes	EXEC Privilege
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

configure

Enter CONFIGURATION mode from EXEC Privilege mode.

Syntax	`configure [terminal]`
Parameters	**terminal** (OPTIONAL) Enter the keyword `terminal` to specify that you are configuring from the terminal.
Command Modes	EXEC Privilege
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#configure
Dell(conf)#
```

debug cpu-traffic-stats

Enable the collection of computer processor unit (CPU) traffic statistics.

Syntax	`debug cpu-traffic-stats`
Defaults	Disabled
Command Modes	EXEC Privilege
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	This command enables (and disables) the collection of CPU traffic statistics from the time this command is executed (not from system boot). However, excessive traffic a CPU receives automatically triggers (turn on) the collection of CPU traffic statics.

The following message is an indication that collection of CPU traffic is automatically turned on. To view the traffic statistics, use the `show cpu-traffic-stats` command.

If the CPU receives excessive traffic, traffic is rate controlled.

NOTE: You must enable this command before the `show cpu-traffic-stats` command displays traffic statistics. Dell Networking OS recommends disabling debugging (`no debug cpu-traffic-stats`) after troubleshooting is complete.

Related Commands: show cpu-traffic-stats — displays the cpu traffic statistics.

debug ftpserver

View transactions during an FTP session when a user is logged into the FTP server.

Syntax: `debug ftpserver`

Command Modes: EXEC Privilege

Command History:

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

disable

Return to EXEC mode.

Syntax: `disable [level]`

Parameters:

level	(OPTIONAL) Enter a number for a privilege level of the Dell OS. The range is from 0 to 15. The default is **1**.

Defaults: **1**

Command Modes: EXEC Privilege

Command History:

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

do

Allows the execution of most EXEC-level commands from all CONFIGURATION levels without returning to the EXEC level.

Syntax `do command`

Parameters

command	Enter an EXEC-level command.

Defaults none

Command Modes

- CONFIGURATION
- INTERFACE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information The following commands are *not* supported by the `do` command:

- `enable`
- `disable`
- `exit`
- `config`

Example

```
Dell(conf-if-te-5/0)#do clear counters
Clear counters on all interfaces [confirm]
Dell(conf-if-te-5/0)#
Dell(conf-if-te-5/0)#do clear logging
Clear logging buffer [confirm]
Dell(conf-if-te-5/0)#
Dell(conf-if-te-5/0)#do reload
System configuration has been modified. Save? [yes/no]: n
Proceed with reload [confirm yes/no]: n
Dell(conf-if-te-5/0)#
```

enable

Enter EXEC Privilege mode or any other privilege level configured. After entering this command, you may need to enter a password.

Syntax `enable [level]`

Parameters

level	(OPTIONAL) Enter a number for a privilege level of the Dell Networking OS. The range is from 0 to 15. The default is **15**.

Defaults **15**

Command Modes	EXEC
Command History	

Version 9.5(0.0)	Introduced the support for roles on the MXL 10/40GbE Switch.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Users entering EXEC Privilege mode or any other configured privilege level can access configuration commands. To protect against unauthorized access, use the `enable password` command to configure a password for the `enable` command at a specific privilege level. If no privilege level is specified, the default is privilege level **15**.

NOTE: If you are authorized for the EXEC privilege mode by your role, you do not need to enter an enable password.

Related Commands

enable password — configures a password for the `enable` command and to access a privilege level.

enable optic-info-update interval

Enable polling intervals of optical information updates for simple network management protocol (SNMP).

Syntax

`enable optical-info-update interval` *`seconds`*

To disable optical power information updates, use the `no enable optical-info-update interval` command.

Parameters

interval *seconds*	Enter the keyword `interval` then the polling interval in seconds. The range is from 120 to 6000 seconds. The default is **300 seconds** (5 minutes).

Defaults	Disabled
Command Modes	CONFIGURATION
Command History	Version 8.3.16.1 — Replaces the `enable xfp-power-updates` command.
Usage Information	To enable polling and to configure the polling frequency, use this command.

end

Return to EXEC Privilege mode from other command modes (for example, CONFIGURATION or ROUTER OSPF modes).

Syntax

```
end
```

Command Modes

- CONFIGURATION
- SPANNING TREE
- MULTIPLE SPANNING TREE
- LINE
- INTERFACE
- VRRP
- ACCESS-LIST
- PREFIX-LIST
- ROUTER OSPF
- ROUTER RIP

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

exit — returns to the lower command mode.

exec-banner

Enable the display of a text string when the user enters EXEC mode.

Syntax

```
exec-banner
```

Defaults

Enabled on all lines (if configured, the banner appears).

Command Modes

LINE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Optionally, use the `banner exec` command to create a text string that is displayed when you access EXEC mode. This command toggles that display.

Related Commands

banner exec — configures a banner to display when entering EXEC mode.

line — enables and configures console and virtual terminal lines to the system.

exec-timeout

Set a time interval that the system waits for input on a line before disconnecting the session.

Syntax

```
exec-timeout minutes [seconds]
```

To return to default settings, use the `no exec-timeout` command.

Parameters

minutes	Enter the number of minutes of inactivity on the system before disconnecting the current session. The range is from 0 to 35791. The default is **10 minutes** for the console line and **30 minutes** for the VTY line.
seconds	(OPTIONAL) Enter the number of seconds. The range is from 0 to 2147483. The default is **0 seconds**.

Defaults

10 minutes for console line; **30 minutes** for VTY lines; **0 seconds**

Command Modes

LINE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To remove the time interval, use the `exec-timeout 0 0` command.

Example

```
Dell con0 is now available
Press RETURN to get started.
Dell>
```

exit

Return to the lower command mode.

Syntax

```
exit
```

Command Modes

- EXEC Privilege
- CONFIGURATION
- LINE
- INTERFACE
- PROTOCOL GVRP
- SPANNING TREE
- MULTIPLE SPANNING TREE
- MAC ACCESS LIST
- ACCESS-LIST
- PREFIX-LIST
- ROUTER OSPF

- ROUTER RIP

Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	end — returns to EXEC Privilege mode.

ftp-server enable

Enable FTP server functions on the system.

Syntax	`ftp-server enable`
Defaults	Disabled
Command Modes	CONFIGURATION
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
morpheus% ftp 10.31.1.111
Connected to 10.31.1.111.
220 FTOS (1.0) FTP server ready
Name (10.31.1.111:dch): dch
331 Password required
Password:
230 User logged in
ftp> pwd
257 Current directory is "flash:"
ftp> dir
200 Port set okay
150 Opening ASCII mode data connection
size  date       time name
-------- ------ ------ --------
 512  Jul-20-2004  18:15:00 tgtimg
 512  Jul-20-2004  18:15:00 diagnostic
 512  Jul-20-2004  18:15:00 other
 512  Jul-20-2004  18:15:00 tgt
226 Transfer complete
329 bytes received in 0.018 seconds (17.95 Kbytes/s)
ftp>
```

Related Commands

ftp-server topdir — sets the directory to be used for incoming FTP connections.

ftp-server username — sets a username and password for incoming FTP connections.

ftp-server topdir

Specify the top-level directory to be accessed when an incoming FTP connection request is made.

Syntax

```
ftp-server topdir directory
```

Parameters

directory	Enter the directory path.

Defaults

The internal flash is the default directory.

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

After you enable FTP server functions with the `ftp-server enable` command, Dell Networking OS recommends specifying a top-level directory path. Without a top-level directory path specified, the Dell Networking OS directs users to the flash directory when logging in to the FTP server.

Related Commands

ftp-server enable — enables FTP server functions on the MXL 10/40GbE switch IO module.

ftp-server username — sets a username and password for incoming FTP connections to the MXL 10/40GbE switch IO module.

ftp-server username

Create a user name and associated password for incoming FTP server sessions.

Syntax

```
ftp-server username username password [encryption-type]
password
```

Parameters

username	Enter a text string up to 40 characters long as the user name.
password *password*	Enter the keyword `password` then a string up to 40 characters long as the password. Without specifying an encryption type, the password is unencrypted.
encryption-type	(OPTIONAL) After the keyword `password`, enter one of the following numbers: • `0` (zero) for an unecrypted (clear text) password • `7` (seven) for a hidden text password

Defaults

Not enabled.

Command Modes	CONFIGURATION	
Command History	**Version 8.3.16.1**	Introduced on the MXL 10/40GbE Switch IO Module.

hostname

Set the host name of the system.

Syntax	`hostname` *`name`*	
Parameters	*name*	Enter a text string, up to 32 characters long.
Defaults	Dell	
Command Modes	CONFIGURATION	
Command History	**Version 9.3(0.0)**	Modified the default hostname as Dell.
	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	The hostname is used in the prompt. You cannot specify spaces in the hostname. Starting with Dell Networking OS version 9.3(0.0), the default hostname is modified as Dell instead of FTOS on all of the supported platforms.	

ip ftp password

Specify a password for outgoing FTP connections.

Syntax	`ip ftp password [`*`encryption-type`*`]` *`password`*	
Parameters	*encryption-type*	(OPTIONAL) Enter one of the following numbers: • `0` (zero) for an unecrypted (clear text) password • `7` (seven) for a hidden text password
	password	Enter a string up to 40 characters as the password.
Defaults	Not configured.	
Command Modes	CONFIGURATION	

Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	The password is listed in the configuration file; you can view the password by entering the `show running-config ftp` command in EXEC mode. Use the `ip ftp password` command when you use the `ftp: parameter` in the `copy` command.
Related Commands	copy — copy files. ftp-server username — sets the user name for the FTP sessions.

ip ftp source-interface

Specify an interface's IP address as the source IP address for FTP connections.

Syntax `ip ftp source-interface` *`interface`*

Parameters

interface	Enter the following keywords and slot/port or number information: • For Loopback interfaces, enter the keyword `loopback` then a number from zero (0) to 16383. • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

Defaults	The IP address on the system that is closest to the Telnet address is used in the outgoing packets.
Command Modes	CONFIGURATION
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	copy — copies files from and to the switch.

ip ftp username

Assign a user name for outgoing FTP connection requests.

Syntax	`ip ftp username` *`username`*
Parameters	*username* — Enter a text string as the user name up to 40 characters long.
Defaults	No user name is configured.
Command Modes	CONFIGURATION
Command History	**Version 8.3.16.1** — Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	Configure a password with the `ip ftp password` command.
Related Commands	ip ftp password — sets the password for FTP connections.

ip telnet server enable

Enable the Telnet server on the switch.

Syntax	`ip telnet server enable` To disable the Telnet server, use the `no ip telnet server enable` command.
Defaults	Enabled
Command Modes	CONFIGURATION
Command History	**Version 8.3.16.1** — Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	ip ssh server — enables the secure shell (SSH) server on the system.

ip telnet source-interface

Set an interface's IP address as the source address in outgoing packets for Telnet sessions.

Syntax	`ip telnet source-interface` *`interface`*
Parameters	*interface* — Enter the following keywords and slot/port or number information:

- For Loopback interfaces, enter the keyword `loopback` then a number from zero (0) to 16383.
- For a Port Channel, enter the keywords `port-channel` then a number. The range is from 1 to 128.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

Defaults	The IP address on the system that is closest to the Telnet address is used in the outgoing packets.
Command Modes	CONFIGURATION
Command History	Version 8.3.16.1 — Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	telnet — telnets to another device.

ip tftp source-interface

Assign an interface’s IP address in outgoing packets for TFTP traffic.

Syntax `ip tftp source-interface` *`interface`*

Parameters

interface	Enter the following keywords and slot/port or number information: • For Loopback interfaces, enter the keyword `loopback` then a number from zero (0) to 16383. • For a Port Channel, enter the keywords `port-channel` then a number. The range is 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

Defaults	The IP address on the system that is closest to the Telnet address is used in the outgoing packets.
Command Modes	CONFIGURATION

Command History	**Verison 8.3.16.1**	Introduced on the MXL 10/40GbE Switch IO Module.

line

Enable and configure console and virtual terminal lines to the system. This command accesses LINE mode, where you can set the access conditions for the designated line.

Syntax `line {console 0 | vty number [end-number]}`

Parameters

console 0	Enter the keyword `console 0` to configure the console port. The console option is `<0-0>`.
vty *number*	Enter the keyword `vty` then a number from 0 to 9 to configure a virtual terminal line for Telnet sessions. The system supports 10 Telnet sessions.
end-number	(OPTIONAL) Enter a number from 1 to 9 as the last virtual terminal line to configure. You can configure multiple lines at one time.

Defaults Not configured

Command Modes CONFIGURATION

Command History	**Version 8.3.17.0**	Supported on the M I/O Aggregator.

Usage Information You cannot delete a terminal connection.

Related Commands show memory — view current memory usage on the M I/O Aggregator.

motd-banner

Enable a message of the day (MOTD) banner to appear when you log in to the system.

Syntax `motd-banner`

Defaults Enabled on all lines.

Command Modes LINE

Command History	**Version 8.3.16.1**	Introduced on the MXL 10/40GbE Switch IO Module.

ping

Test connectivity between the system and another device by sending echo requests and waiting for replies.

Syntax

```
ping [host | ip-address | ipv6-address] [count {number |
continuous}] [datagram-size] [timeout] [source (ip src-ipv4-
address) | interface] [tos] [df-bit (y|n)] [validate-reply(y|
n)] [outgoing-interface] [pattern pattern] [sweep-min-size]
[sweep-max-size] [sweep-interval] [ointerface (ip src-ipv4-
address) | interface]
```

Parameters

host	(OPTIONAL) Enter the host name of the devices to which you are testing connectivity.
ip-address	(OPTIONAL) Enter the IPv4 address of the device to which you are testing connectivity. The address must be in the dotted decimal format.
count	Enter the number of echo packets to be sent. The default is **5**. • number: from 1 to 2147483647 • continuous: transmit echo request continuously
datagram size	Enter the ICMP datagram size. The range is from 36 to 15360 bytes. The default is **100**.
timeout	Enter the interval to wait for an echo reply before timing out. The range is from 0 to 3600 seconds. The default is **2 seconds**.
source	Enter the IPv4 or IPv6 source ip address or the source interface. For IPv6 addresses, you may enter global addresses only. Enter the IP address in A.B.C.D format. • For a Port Channel interface, enter the keywords `port-channel` then a number: The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.
tos	(IPv4 only) Enter the type of service required. The range is from 0 to 255. The default is **0**.
df-bit	(IPv4 only) Enter `Y` or `N` for the “don't fragment” bit in IPv4 header. • `N`: Do not set the “don't fragment” bit. • `Y`: Do set “don't fragment” bit Default is **No**.

validate-reply	(IPv4 only) Enter `Y` or `N` for reply validation. • `N`: Do not validate reply data. • `Y`: Do validate reply data. Default is `No`.
pattern *pattern*	(IPv4 only) Enter the IPv4 data pattern. Range: 0-FFFF. Default: **0xABCD**.
sweep-min-size	Enter the minimum size of datagram in sweep range. The range is from 52 to 15359 bytes.
sweep-max-size	Enter the maximum size of datagram in sweep range. The range is from 53 to 15359 bytes.
sweep-interval	Enter the incremental value for sweep size. The range is from 1 to 15308 seconds.
ointerface	(IPv4 only) Enter the outgoing interface for multicast packets. Enter the IP address in A.B.C.D format. • For a Port Channel, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

Defaults

See parameters above.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

When you enter the `ping` command without specifying an IP address (Extended Ping), you are prompted for a target IP address, a repeat count, a datagram size (up to 1500 bytes), a timeout (in seconds), and for Extended Commands. For information on the ICMP message codes that return from a `ping` command, refer to Internet Control Message Protocol (ICMP) Message Types.

Example (IPv4)

```
Dell#ping 172.31.1.255

Type Ctrl-C to abort.

Sending 5, 100-byte ICMP Echos to 172.31.1.255, timeout is 2
seconds:
Reply to request 1 from 172.31.1.208 0 ms
Reply to request 1 from 172.31.1.216 0 ms
Reply to request 1 from 172.31.1.205 16 ms
::
```

```
Reply to request 5 from 172.31.1.209 0 ms
Reply to request 5 from 172.31.1.66 0 ms
Reply to request 5 from 172.31.1.87 0 ms
Dell#
```

Example (IPv6)

```
Dell#ping 100::1

Type Ctrl-C to abort.

Sending 5, 100-byte ICMP Echos to 100::1, timeout is 2 seconds:
!!!!!
Success rate is 100.0 percent (5/5), round-trip min/avg/max =
0/0/0 (ms)
Dell#
```

reload

Reboot the Dell Networking OS.

Syntax `reload`

Command Modes EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information If there is a change in the configuration, the Dell Networking OS prompts you to save the new configuration. Or you can save your running configuration with the `copy running-config` command.

Related Commands redundancy disable-auto-reboot — Resets any designated stack member except the management unit.

send

Send messages to one or all terminal line users.

Syntax `send [*] | [line ] | [console] | [vty]`

Parameters

*	Enter the asterisk character `*` to send a message to all tty lines.
line	Send a message to a specific line. The range is from 0 to 11.
console	Enter the keyword `console` to send a message to the primary terminal line.
vty	Enter the keyword `vty` to send a message to the virtual terminal.

Defaults	none
Command Modes	EXEC
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	Messages can contain an unlimited number of lines; however, each line is limited to 255 characters. To move to the next line, use `<CR>`. To send the message use `CTR-Z`; to abort a message, use `CTR-C`.

service timestamps

To debug and log messages, add time stamps. This command adds either the uptime or the current time and date.

Syntax

```
service timestamps [debug | log] [datetime [localtime] [msec]
[show-timezone] | uptime]
```

Parameters

debug	(OPTIONAL) Enter the keyword `debug` to add timestamps to debug messages.
log	(OPTIONAL) Enter the keyword `log` to add timestamps to log messages with severity from 0 to 6.
datetime	(OPTIONAL) Enter the keyword `datetime` to have the current time and date added to the message.
localtime	(OPTIONAL) Enter the keyword `localtime` to include the localtime in the timestamp.
msec	(OPTIONAL) Enter the keyword `msec` to include milliseconds in the timestamp.
show-timezone	(OPTIONAL) Enter the keyword `show-timezone` to include the time zone information in the timestamp.
uptime	(OPTIONAL) Enter the keyword `uptime` to have the timestamp based on time elapsed since system reboot.

Defaults	Not configured.
Command Modes	CONFIGURATION
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	If you do not specify parameters and enter `service timestamps`, it appears as `service timestamps debug uptime` in the running-configuration.

To view the current options set for the `service timestamps` command, use the `show running-config` command.

show alarms

View alarms.

Syntax	`show alarms`
Command Modes	• EXEC • EXEC Privilege
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell# show alarms

-- Minor Alarms --
Alarm Type                 Duration
---------------------------------------
No minor alarms

-- Major Alarms --
Alarm Type                 Duration
----------------------------------------
No major alarms

Dell#
```

show command-history

Display a buffered log of all commands all users enter along with a time stamp.

Syntax	`show command-history`
Defaults	none
Command Modes	• EXEC • EXEC Privilege
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	One trace log message is generated for each command. No password information is saved to this file.

Example

```
Dell#show command-history
[4/20 10:27:23]: CMD-(CLI):[enable]by default from console
```

```
[4/20 10:27:23]: CMD-(CLI):[configure terminal]by default from
console
     - Repeated 1 time.
[4/20 10:27:23]: CMD-(CLI):[snmp-server community public ro]by
default from
console
[4/20 10:27:23]: CMD-(CLI):[logging 172.16.1.162]by default
from console
[4/20 10:27:23]: CMD-(CLI):[logging 10.10.10.4]by default from
console
[4/20 10:27:24]: CMD-(CLI):[logging 10.1.2.4]by default from
console
[4/20 10:27:24]: CMD-(CLI):[logging 172.31.1.4]by default from
console
[4/20 10:27:24]: CMD-(CLI):[logging 133.33.33.4]by default
from console
[4/20 10:27:24]: CMD-(CLI):[management route 172.16.1.0 /24
10.11.209.4]by default
from console
[4/20 10:27:24]: CMD-(CLI):[service timestamps log datetime]by
default from
console
[4/20 10:27:24]: CMD-(CLI):[line console 0]by default from
console
[4/20 10:27:24]: CMD-(CLI):[exec-timeout 0]by default from
console
[4/20 10:27:24]: CMD-(CLI):[exit]by default from console
[4/20 10:27:29]: CMD-(CLI):[show version]by default from
console
[4/20 10:27:56]: CMD-(CLI):[show interfaces tengigabitethernet
0/3]by default from
console
[4/20 10:55:8]: CMD-(CLI):[show lldp neighbors]by default from
console
[4/20 15:17:6]: CMD-(CLI):[show cam-acl]by default from console
[4/20 16:34:59]: CMD-(CLI):[show running-config interface
tengigabitethernet 0/
55]by default from console
[4/20 16:38:14]: CMD-(CLI):[show vlan]by default from console
[5/4 9:11:52]: CMD-(TEL0):[show version]by admin from vty0
(10.11.68.14)
[5/4 9:12:9]: CMD-(TEL0):[show hosts]by admin from vty0
(10.11.68.14)
[5/4 9:14:38]: CMD-(TEL0):[show arp]by admin from vty0
(10.11.68.14)
[5/4 9:19:29]: CMD-(TEL0):[enable]by admin from vty0
(10.11.68.14)
[5/4 9:19:35]: CMD-(TEL0):[configure]by admin from vty0
(10.11.68.14)
     - Repeated 1 time.
[5/4 9:19:50]: CMD-(TEL0):[interface tengigabitethernet
0/16]by admin from vty0
(10.11.68.14)
[5/4 9:20:11]: CMD-(TEL0):[exit]by admin from vty0
(10.11.68.14)
Dell#
```

Related Commands	clear command history — clears the command history log.

show command-tree

Display the entire CLI command tree, and optionally, display the utilization count for each command and its options.

Syntax

`show command-tree [count | no]`

Parameters

count	Display the command tree with a usage counter for each command.
no	Display all of the commands that may be preceded by the keyword `no`, which is the keyword used to remove a command from the running-configuration.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Reload the system to reset the command-tree counters.

Example

```
Dell#show command-tree count
!
Enable privilege mode:
calendar             command usage:5
set                    option usage: 0
hh:mm:ss               option usage: 0
<1-31>                 option usage: 0
<MONTH>                option usage: 0
<1993-2035>            option usage: 0
<MONTH>                option usage: 0
<1-31>                 option usage: 0
<1993-2035>            option usage: 0

clear arp-cache       command usage:2

clear ip dhcp         command usage:1
binding                 option usage: 0
A.B.C.D                 option usage: 0
client                  option usage: 0
 statistics             option usage: 0
  interface             option usage: 0
   fastethernet         option usage: 0
    SLOT/PORT           option usage: 0
   fortyGigE            option usage: 0
    SLOT/PORT           option usage: 0
    SLOT/PORT           option usage: 0
   managementethernet   option usage: 0
    SLOT/PORT           option usage: 0
   port-channel         option usage: 0
   <1-128>              option usage: 0
   tengigabitethernet   option usage: 0
    SLOT/PORT           option usage: 0
   vlan                 option usage: 0
   <1-4094>             option usage: 0
 conflict               option usage: 0
  A.B.C.D               option usage: 0
 server                 option usage: 0
   statistics           option usage: 0
  snooping              option usage: 0
   binding              option usage: 0

clear ip fib         command usage:4

clear ip route       command usage:1
Dell#
```

show cpu-traffic-stats

View the CPU traffic statistics.

Syntax

```
show cpu-traffic-stats [port number | all]
```

Parameters

port number	(OPTIONAL) Enter the port number to display traffic statistics on that port only. The range is from 1 to 1568.
all	(OPTIONAL) Enter the keyword `all` to display traffic statistics on all the interfaces receiving traffic, sorted based on the traffic.

Defaults **all**

Command Modes EXEC

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Traffic statistics are sorted on a per-interface basis; the interface receiving the most traffic is displayed first. All CPU and port information is displayed unless a specific port or CPU is specified. Traffic information is displayed for router ports only; not for management interfaces. The traffic statistics are collected only after the `debug cpu-traffic-stats` command is executed; not from the system bootup.

NOTE: After debugging is complete, use the `no debug cpu-traffic-stats` command to shut off traffic statistics collection.

Example

```
Dell#show cpu-traffic-stats
Processor : CP
--------------
  Received 100% traffic on TenGigabitEthernet 8/2 Total
packets:100
    LLC:0, SNAP:0, IP:100, ARP:0, other:0
    Unicast:100, Multicast:0, Broadcast:0
Dell#
```

Related Commands	debug cpu-traffic-stats — enables CPU traffic statistics for debugging.

show debugging

View a list of all enabled debugging processes.

Syntax	`show debugging`
Command Modes	EXEC Privilege
Command History	Version 8.3.16.1 — Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show debug
Generic IP: (Access List: test)
  IP packet debugging is on for (Access List: test)
    TenGigabitEthernet 0/16
  ICMP packet debugging is on for
    TenGigabitEthernet 0/16
OSPF:1
    OSPF packet debugging is on
DHCP:
    DHCP debugging is on
Dell#
```

show environment

View system component status (for example, temperature or voltage).

Syntax

`show environment [all | stack-unit unit-id]`

Parameters

all	Enter the keyword `all` to view all components.
stack-unit *unit-id*	Enter the keyword `stack-unit` then the unit-id to display information on a specific stack member. The range is from 0 to 5.
thermal sensor	Enter the keywords `thermal-sensor` to view all components.

Command Modes

- EXEC
- EXEC Privildge

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following example shows the output of the `show environment fan` command as it appears prior to the Dell Networking OS version 7.8.1.0.

Example (all)

```
Dell#show environment all

-- Unit Environment Status --
Unit  Status    Temp    Voltage
-------------------------------------------
* 0   online    47C     ok

* Management Unit

-- Thermal Sensor Readings (deg C) --
Unit Sensor0 Sensor1 Sensor2 Sensor3 Sensor4 Sensor5 Sensor6
Sensor7
Sensor8 Sensor9
---------------------------------------------------------------
-----
----------------
0    50     52       53      53      54      48       57     57
53   56
Dell#
```

Example (stack-unit)

```
Dell#show environment stack-unit 0

-- Unit Environment Status --
Unit   Status    Temp    Voltage
------------------------------------
0*     online    49C     ok

* Management Unit
```

Example (thermal-sensor)

```
Dell#show environment thermal-sensor

-- Thermal Sensor Readings (deg C) --
Unit Sensor0 Sensor1 Sensor2 Sensor3 Sensor4 Sensor5 Sensor6
Sensor7
Sensor8 Sensor9
---------------------------------------------------------------
----
----------------
0    50      52      53      53      54      48      57
5753   56

* Management Unit
Dell#
```

show inventory

Display the switch type, components (including media), and Dell Networking OS version including hardware identification numbers and configured protocols.

Syntax `show inventory [media slot]`

Parameters

media *slot*	(OPTIONAL) Enter the keyword `media` then the stack ID of the stack member you want to display pluggable media inventory.

Defaults

none

Command Modes

EXEC

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

If there are no fiber ports in the unit, just the header under `show inventory media` displays. If there are fiber ports but no optics inserted, the output displays "Media not present or accessible".

Example

```
Dell#show inventory
System Type      : MXL-10/40GbE
System Mode      : 1.0
Software Version : NAVASOTA-DEV-9-1-0-917
Unit Type          Serial Number   Part Number Revision
--------------------------------------------------------------
* 1  MXL-10/40GbE  TW282921F00048  0NVH81      2.0
* - Management Unit

Software Protocol Configured
--------------------------------------------------------------
  SNMP
  LLDP
Dell#
```

Example (media)

```
Dell#show inv media
Slot Port Type  Media          Serial Number   F10Qualid
----------------------------------------------------------
0    33   QSFP  40GBASE-CR4-1M APF11490011J2Q  Yes
0    37   QSFP  40GBASE-SR4    MLJ004V         No
0    41   QSFP  40GBASE-SR4    MLJ003P         No
0    42   QSFP  40GBASE-SR4    MLJ003P         No
0    43   QSFP  40GBASE-SR4    MLJ003P         No
0    44   QSFP  40GBASE-SR4    MLJ003P         No
0    45   QSFP  40GBASE-SR4    MLJ004Y         No
0    46   QSFP  40GBASE-SR4    MLJ004Y         No
0    47   QSFP  40GBASE-SR4    MLJ004Y         No
0    48   QSFP  40GBASE-SR4    MLJ004Y         No
0    49       Media not present or accessible
0    50       Media not present or accessible
0    51       Media not present or accessible
0    52       Media not present or accessible
0    53   QSFP  40GBASE-SR4   MK50012          No
0    54   QSFP  40GBASE-SR4   MK50012          No
0    55   QSFP  40GBASE-SR4   MK50012          No
0    56   QSFP  40GBASE-SR4   MK50012          No
Dell#
```

Related Commands

show interfaces — displays a specific interface configuration.

show interfaces transceiver — displays the physical status and operational status of an installed transceiver. The output also displays the transceiver's serial number.

show memory

View current memory usage on the MXL switch.

Syntax	`show memory [stack-unit 0–5]`
Parameters	**stack-unit *0–5*** (OPTIONAL) Enter the keywords `stack-unit` then the stack unit ID of the stack member to display memory information on the designated stack member.
Command Modes	EXEC EXEC Privilege
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	The output for `show memory` displays the memory usage of LP part (sysdlp) of the system. The sysdlp is an aggregate task that handles all the tasks running on the CPU.

Example

```
Dell#show memory stack-unit 0
  Statistics On Unit 0 Processor
  ===========================
Total(b)   Used(b)  Free(b)    Lowest(b)  Largest(b)
268435456  4010354  264425102  264375410  264425102
```

show processes cpu

Display CPU usage information based on processes running.

Syntax

`show processes cpu [management-unit 1-99 [details] | stack-unit 0–5 | summary | ipc | memory [stack-unit 0–5]]`

Parameters

management-unit *1-99* [details]	(OPTIONAL) Display processes running in the control processor. The `1-99` variable sets the number of tasks to display in order of the highest CPU usage in the past five (5) seconds. Add the keyword `details` to display all running processes (except sysdlp). Refer to Example (management-unit).
stack-unit *0–5*	(OPTIONAL) Enter the keyword `stack-unit` then the stack member ID. The range is from 0 to 5.

As an option of the `show processes cpu` command, this option displays CPU usage for the designated stack member. Or, as an option of `memory`, this option limits the output of memory statistics to the designated stack member. Refer to Example (stack-unit).

summary	(OPTIONAL) Enter the keyword `summary` to view the CPU utilization of processes related to line card processing.
ipc	(OPTIONAL) Enter the keyword `ipc` to display interprocess communication statistics.
memory	(OPTIONAL) Enter the keyword `memory` to display memory statistics. Refer to Example (memory).

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example (summary)

```
Dell#show processes cpu summary
CPU utilization  5Sec   1Min  5Min
-------------------------------------------
Unit0            0%     0%     0%

CPU utilization 5Sec    1Min  5Min
-------------------------------------------
Unit1*          1%      0%    0%
Unit2           0%      0%    0%
Unit3           0%      0%    0%
* Mgmt Unit
```

Example (management-unit)

```
Dell#show proc cpu management-unit 5
CPU utilization for five seconds: 6%/0%; one minute: 6%; five
minutes: 7%
PID         Runtime(ms) Invoked  uSecs  5Sec  1Min  5Min  TTY
Process
0x00000000  4650        465      10000  4.43% 4.43% 4.43% 0
system
0x00000112  56372590    5637259  10000  1.58% 1.78% 1.89% 0
sysdlp
0x00000107  9630080     963008   10000  0.79% 0.28% 0.33% 0
sysd
0x00000172  1435540     143554   10000  0.00% 0.10% 0.05% 0
igmp
0x000001fc  1366570     136657   10000  0.00% 0.08% 0.05% 0
frrp
Dell#
```

Example (stack-unit)

```
Dell#show process cpu stack-unit 0
CPU utilization for five seconds: 4%/0%; one minute: 3%; five
minutes: 2%
PID        Runtime(ms) Invoked uSecs 5Sec  1Min 5Min   TTY
Process
0x763a7000 96806080    9680608 10000 3.00% 3.25% 2.93% 0
KP
```

```
0x760d5000 26384050    2638405 10000 1.00% 0.50% 0.32% 0
frrpagt
0x762da000 491370      49137   10000 0.00% 0.00% 0.00% 0
F10StkMgr
0x762f9000 665580      66558   10000 0.00% 0.00% 0.00% 0
lcMgr
0x7631d000 37580       3758    10000 0.00% 0.00% 0.00% 0
dla
0x76348000 452110      45211   10000 0.00% 0.00% 0.00% 0
sysAdmTsk
0x76367000 1751990     175199  10000 0.00% 0.00% 0.00% 0
timerMgr
0x76385000 14460       1446    10000 0.00% 0.00% 0.00% 0
PM
0x7629d000 347970      34797   10000 0.00% 0.00% 0.00% 0
diagagt
0x763c7000 0           0       0     0.00% 0.00% 0.00% 0
evagt
0x763eb000 90800       9080    10000 0.00% 0.00% 0.00% 0
ipc
0x77ee9000 5           0    5 1 0000 0.00% 0.00% 0.00% 0
tme
0x77eec000 0           0           0 0.00% 0.00% 0.00% 0
ttraceIpFlow
0x77eee000 20          2       10000 0.00% 0.00% 0.00% 0
linkscan_user_threa
0x77ff6000 0           0           0 0.00% 0.00% 0.00% 0
isrTask
0x7811a000 0           0           0 0.00% 0.00% 0.00% 0
tDDB
0x7811c000 22980       2298    10000 0.00% 0.00% 0.00% 0
GC
0x7811e000 0           0           0 0.00% 0.00% 0.00% 0
bshell_reaper_threa
0x78365000 10          1       10000 0.00% 0.00% 0.00% 0
tSysLog
0x78367000 1106980     110698  10000 0.00% 0.00% 0.00% 0
tTimerTask
0x78369000 13131160    1313116 10000 0.00% 0.08% 0.00% 0
tExcTask
0x7836b000 30          3       10000 0.00% 0.00% 0.00% 0
tLogTask
0x785bb000 147650      14765   10000 0.00% 0.00% 0.00% 0
tUsrRoot
```

Example (memory)

```
Dell#show processes memory

Memory Statistics Of Stack Unit 0 (bytes)
===========================================================
Total: 2147483648, MaxUsed: 378417152, CurrentUsed: 378417152,
CurrentFree:
1769066496
  TaskName TotalAllocated TotalFreed MaxHeld CurrentHolding
  f10appioserv     225280          0       0      208896
          ospf     573440          0       0     8716288
  f10appioserv     225280          0       0      208896
     fcoecntrl     262144          0       0     7917568
      dhclient     548864          0       0     1310720
  f10appioserv     225280          0       0      208896
          ndpm     618496          0       0     7512064
  f10appioserv     225280          0       0      208896
          vrrp     335872          0       0     8048640
  f10appioserv     225280          0       0      208896
```

```
          frrp     180224         0        0     7512064
  f10appioserv     225280         0        0      208896
          xstp    2740224         0        0     9801728
  f10appioserv     225280         0        0      208896
           pim    1007616         0        0     7757824
  f10appioserv     225280         0        0      208896
          igmp     401408         0        0     7639040
  f10appioserv     225280         0        0      208896
          mrtm    5496832         0        0    11124736
  f10appioserv     225280         0        0      208896
         l2mgr    1036288         0        0    16134144
  f10appioserv     225280         0        0      208896
          l2pm     172032         0        0     7483392
  f10appioserv     225280         0        0      208896
          arpm     192512         0        0     7057408
Dell#
```

Example (stack-unit)

```
Dell#show process memory stack-unit 0
Total: 2147483648, MaxUsed: 378433536, CurrentUsed: 378433536,
CurrentFree:
1769050112
  TaskName     TotalAllocated TotalFreed MaxHeld CurrentHolding
  f10appioserv         225280          0       0       208896
          ospf         573440          0       0      8716288
  f10appioserv         225280          0       0       208896
     fcoecntrl         262144          0       0      7917568
      dhclient         548864          0       0      1310720
  f10appioserv         225280          0       0       208896
          ndpm         618496          0       0      7512064
  f10appioserv         225280          0       0       208896
          vrrp         335872          0       0      8048640
  f10appioserv         225280          0       0       208896
          frrp         180224          0       0      7512064
  f10appioserv         225280          0       0       208896
          xstp        2740224          0       0      9801728
  f10appioserv         225280          0       0       208896
           pim        1007616          0       0      7757824
  f10appioserv         225280          0       0       208896
Dell#
```

Related Commands

show hardware layer2 acl — displays Layer 2 ACL data for the selected stack member and stack member port-pipe.

show hardware layer3 — displays Layer 3 ACL or QoS data for the selected stack member and stack member port-pipe.

show hardware stack-unit — displays the data plane or management plane input and output statistics of the designated component of the designated stack member.

show hardware system-flow — displays Layer 3 ACL or QoS data for the selected stack member and stack member port-pipe.

show interfaces stack-unit — displays information on all interfaces on a specific stack member.

show processes memory — displays CPU usage information based on processes running.

show processes ipc flow-control

Display the single window protocol queue (SWPQ) statistics.

Syntax

`show processes ipc flow-control [cp]`

Parameters

cp	(OPTIONAL) Enter the keyword `cp` to view the control processor's SWPQ statistics.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Field	Description
Source QID /Tx Process	Source Service Identifier
Destination QID/Rx Process	Destination Service Identifier
Cur Len	Current number of messages enqueued
High Mark	Highest number of packets in the queue at any time
#of to / Timeout	Timeout count
#of Retr /Retries	Number of retransmissions
#msg Sent/Msg Sent/	Number of messages sent
#msg Ackd/Ack Rcvd	Number of messages acknowledged
Retr /Available Retra	Number of retries left
Total/ Max Retra	Number of retries allowed

Important Points:

- The SWP provides flow control-based reliable communication between the sending and receiving software tasks.
- A sending task enqueues messages into the SWP queue3 for a receiving task and waits for an acknowledgement.

- If no response is received within a defined period of time, the SWP timeout mechanism resubmits the message at the head of the FIFO queue.
- After retrying a defined number of times, the `SWP-2-NOMORETIMEOUT` timeout message is generated.
- In the example, a retry (Retries) value of zero indicates that the SWP mechanism reached the maximum number of retransmissions without an acknowledgement.

Example

```
Dell#show processes ipc flow-control

Q Statistics on CP Processor
 TxProcess RxProcess Cur High Time Retr Msg  Ac k Aval Max
                     Len Mark Out  ies Sent Rcvd Retra Retra
      ACL0      RTM0   0    0   0    0    0    0   10    10
      ACL0 DIFFSERV0   0    0   0    0    0    0   10    10
      ACL0     IGMP0   0    0   0    0    0    0   10    10
      ACL0      PIM0   0    0   0    0    0    0   10    10
   ARPMGR0     MRTM0   0    0   0    0    0    0  100   100
     LACP0    IFMGR0   0    0   0    0    0    0   25    25
      RTM0      OTM0   0    0   0    0    0    0   60    60
      RTM0      OTM0   0    0   0    0    0    0   60    60
Dell#
```

show processes memory

Display memory usage information based on the running processes.

Syntax

```
show processes memory {management-unit | stack unit {0–5 | all
| summary}}
```

Parameters

management-unit	Enter the keyword `management-unit` for CPU memory usage of the stack management unit.
stack unit *0–5*	Enter the keyword `stack unit` then a stack unit ID of the member unit for which to display memory usage on the forwarding processor.
all	Enter the keyword `all` for detailed memory usage on all stack members.
summary	Enter the keyword `summary` for a brief summary of memory availability and usage on all stack members.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

show processes memory output Field	Description
Total:	Total system memory available
MaxUsed:	Total maximum memory used ever (history indicated with time stamp)
CurrentUsed:	Total memory currently in use
CurrentFree:	Total system memory available
SharedUsed:	Total used shared memory
SharedFree:	Total free shared memory
PID	Process ID
Process	Process Name
ResSize	Actual resident size of the process in memory
Size	Process test, stack, and data size
Allocs	Total dynamic memory allocated
Frees	Total dynamic memory freed
Max	Maximum dynamic memory allocated
Current	Current dynamic memory in use

The output for the `show process memory` command displays the memory usage statistics running on CP part (sysd) of the system. The sysd is an aggregate task that handles all the tasks running on the MXL 10/40GbE Switch IO Module's CP.

The output of the `show memory` command and this command differ based on which the Dell OS processes are counted.

- In the `show memory` output, the memory size is equal to the size of the application processes.
- In the output of this command, the memory size is equal to the size of the application processes plus the size of the system processes.

Example

```
Dell#show processes memory stack-unit 0
Total: 2147483648, MaxUsed: 378433536, CurrentUsed: 378433536,
CurrentFree:
1769050112
    TaskName TotalAllocated TotalFreed MaxHeld CurrentHolding
f10appioserv         225280          0       0       208896
        ospf         573440          0       0      8716288
f10appioserv         225280          0       0       208896
   fcoecntrl         262144          0       0      7917568
    dhclient         548864          0       0      1310720
f10appioserv         225280          0       0       208896
        ndpm         618496          0       0      7512064
f10appioserv         225280          0       0       208896
        vrrp         335872
```

Example (management-unit)

```
Dell#show processes memory management-unit
Total      : 2147483648, MaxUsed    : 378470400 [05/23/2012
09:49:39]
CurrentUsed:  378470400, CurrentFree: 1769013248
SharedUsed :   18533952, SharedFree : 2437592

PID Process     ResSize    Size  Allocs  Frees   Max
Current
  472 ospf      8716288  573440   94952      0  94952
94952
  529 fcoecntrl 7917568  262144  916736 844764 187920
71972
  225 dhclient  1310720  548864       0             0
0 0
  360 ndpm      7512064  618496    4848      0   4848
4848
  160 vrrp      8048640 3 35872   83700      0  83700
83700
  508 frrp      7512064  180224 1445898 1341684 137342
104214
  186 xstp      9801728 2740224   54986   16564  38422
38422
  374 pim       7757824 1007616  111860       0 111860
111860
--More--
```

show software ifm

Display interface management (IFM) data.

Syntax

show software ifm {clients [summary] | ifagt *number* | ifcb *interface* | stack-unit *unit-ID* | trace-flags}

Parameters

clients	Enter the keyword `clients` to display IFM client information.
summary	(OPTIONAL) Enter the keyword `summary` to display brief information about IFM clients.
ifagt *number*	Enter the keyword `ifagt` then the number of an interface agent to display software pipe and IPC statistics.
ifcb *interface*	Enter the keyword `ifcb` then one of the following interface IDs then the slot/port information to display interface control block information for that interface: • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10G Ethernet interface, enter the keyword `TenGigabitEthernet`. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE`.

stack-unit *unit-ID*	Enter the keywords `stack-unit` then the stack member number to display IFM information for that unit. The range is from 0 to 5.
trace-flags	Enter the keyword `trace-flags` to display IFM information for internal trace flags.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
DELL#show software ifm clients summary
ClntType Inst svcMask    subSvcMask tlvSvcMask tlvSubSvc swp
IPM      0    0x00000000 0x00000000 0x90ff71f3 0xb98784a1 22
RTM      0    0x00000000 0x00000000 0x800010ff 0x0064c798 56
RIP      0    0x00000dfe 0x00000000 0x00000000 0x00000000 0
ISIS     0    0x00000002 0x00000000 0x00000000 0x00000000 0
VRRP     0    0x00000000 0x00000000 0x803330f3 0x0013c480 38
L2PM     0    0x00000000 0x00000000 0x87ff79ff 0xdb80c800 64
ACL      0    0x00000000 0x00000000 0x867f50c3 0x0103c018 81
OSPF     0    0x00000dfa 0x00100338 0x00000000 0x00000000 0
PIM      0    0x000e00f3 0x0000c000 0x00000000 0x00000000 0
IGMP     0    0x000e027f 0x00000000 0x00000000 0x00000000 0
SNMP     0    0x00000000 0x00000000 0x8000c2c0 0x00000002 21
EVTTERM  0    0x00000000 0x00000000 0x800002c0 0x0003c000 20
MRTM     0    0x00000000 0x00000000 0x81f7103f 0xc0600000 30
DSM      0    0x00000000 0x00000000 0x80771033 0x00000000 58
Mirror   0    0x00000000 0x00000000 0x80770003 0x00000000 25
LACP     0    0x00000000 0x00000000 0x8000383f 0x01000000 33
SFL_CP   0    0x00000000 0x00000000 0x807739ff 0x00000000 24
DHCP     0    0x00000000 0x00000000 0x807040f3 0x18001000 35
V6RAD    0    0x00000433 0x0000c000 0x00000000 0x00000000 0
Unidentified Client0   0x006e0002 0x00000000 0x00000000
0x00000000 0
Unidentified Client0   0x6066003f 0x00000000 0x6066003f
0x00000000 95
LLDP     0  0x007f2433 0x0408c000 0x007f2433 0x0408c000 60
--More--
```

show system

Display the current status of all stack members or a specific member.

Syntax `show system [brief | stack-unit unit-id]`

Parameters

brief	(OPTIONAL) Enter the keyword `brief` to view an abbreviated list of system information.

stack-unit *unit-id*	(OPTIONAL) Enter the keyword `stack-unit` then the stack member ID for information on that stack member. The range is 0 to 5.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example (brief)

```
Dell#show system brief

Stack MAC : 00:1e:c9:f1:03:1a

Reload Type : normal-reload [Next boot : normal-reload]
-- Stack Info --
Unit UnitType   Status   ReqTyp       CurTyp       Version Ports
----------------------------------------------------------

0   Member      not present
1   Management  online   MXL-10/40GbE MXL-10/40GbE 9-1-0-917 56
2   Member      not present
3   Member      not present
4   Member      not present
5   Member      not present

Dell#
```

Example (stack-unit)

```
Dell#show system stack-unit 0

-- Unit 0 --
Unit Type       : Management Unit
Status          : online
Next Boot       : online
Required Type   : MXL-10/40GbE - 34-port GE/TE/FG (XL)
Current Type    : MXL-10/40GbE - 34-port GE/TE/FG (XL)
Master priority : 0
Hardware Rev    : X01
Num Ports       : 56
Up Time         : 3 hr, 35 min
FTOS Version    : 8-3-16-160
Jumbo Capable   : yes
POE Capable     : no
Boot Flash      : A: 4.0.1.0bt1 B: 4.0.1.0bt1 [booted]
Boot Selector   : 4.0.0.0bt1
Memory Size     : 2147483648 bytes
Temperature     : 44C
Voltage         : ok
Switch Power    : GOOD
Product Name    : Force10 MXL 10/40GbE
Mfg By          : DELL
Mfg Date        : 2012-01-05
Serial Number   : DELL123456
Part Number     : 0NVH81X01
Piece Part ID   : N/A
PPID Revision   : N/A
Service Tag     : N/A
Expr Svc Code   : N/A
Chassis Svce Tag: RTWB200
```

```
Fabric Id        : C2
Asset tag        : test
PSOC FW Rev      : 0xb
ICT Test Date    : 0-0-0
ICT Test Info    : 0x0
Max Power Req    : 31488
Fabric Type      : 0x3
Fabric Maj Ver   : 0x1
Fabric Min Ver   : 0x0
SW Manageability: 0x4
HW Manageability: 0x1
Max Boot Time    : 6 minutes
Link Tuning      : unsupported
Auto Reboot      : enabled
Burned In MAC    : 00:01:e8:43:de:e1
No Of MACs       :3
```

Related Commands

asset-tag — Assigns and stores a unique asset-tag to the stack member.

show version — Displays the Dell Networking OS version.

show processes memory — Displays memory usage based on running processes.

show system stack-ports — Displays information about the stack ports on all switches in the stack.

show hardware stack-unit — Displays the data plane and management plane input and output statistics of a particular stack member.

stack-unit priority — Configures the ability of the switch to become the management unit of a stack.

show tech-support

Display a collection of data from other show commands, necessary for Dell Networking OS technical support to perform troubleshooting on MXL switches.

Syntax `show tech-support [stack-unit unit-id | page]`

Parameters

stack-unit	(OPTIONAL) Enter the keyword `stack-unit` to view CPU memory usage for the stack member designated by unit-id. The range is 0 to 7.
page	(OPTIONAL) Enter the keyword `page` to view 24 lines of text at a time. Press the SPACE BAR to view the next 24 lines. Press ENTER to view the next line of text. When using the pipe command (|), enter one of these keywords to filter command output. For details about filtering commands, refer to CLI Basics.

save	Enter the keyword `save` to save the command output. flash: Save to local flash drive (`flash://filename` [max 20 chars]).

Command Modes

EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Without the `page` or `stack-unit` option, the command output is continuous. Use Ctrl-z to interrupt the command output.

The `save` option works with other filtering commands. This allows you to save specific information of a `show` command. The `save` entry must always be the last option. For example: `Dell#show tech-support |grep regular-expression |except regular-expression | find regular-expression | save flash://result`

This display output is an accumulation of the same information that is displayed when you execute one of the following `show` commands:

- `show cam`
- `show clock`
- `show environment`
- `show file`
- `show interfaces`
- `show inventory`
- `show ip protocols`
- `show ip route summary`
- `show processes cpu`
- `show processes memory`
- `show redundancy`
- `show running-conf`
- `show version`

Example (partial)

```
Dell#show tech-support ?
page Page through output
stack-unit Unit Number
| Pipe through a command
<cr>
Dell#show tech-support stack-unit 1 ?
page Page through output
| Pipe through a command
<cr>
Dell#show tech-support stack-unit 1 | ?
except Show only text that does not match a pattern
find Search for the first occurrence of a pattern
grep Show only text that matches a pattern
no-more Don't paginate output
save Save output to a file
```

```
Dell#show tech-support stack-unit 1 | save ?
flash: Save to local file system (flash://filename (max 20
chars) )

Dell#show tech-support stack-unit 1 | save flash://LauraSave
Start saving show command report .......
Dell#

Dell#dir
Directory of flash:

Directory of flash:

1 drwx   4096  Jan 01 1980 01:00:00 +01:00 .
2 drwx   2048  May 16 2012 10:49:01 +01:00 ..
3 drwx   4096  Jan 24 2012 19:38:32 +01:00 TRACE_LOG_DIR
4 drwx   4096  Jan 24 2012 19:38:32 +01:00 CORE_DUMP_DIR
5 d---   4096  Jan 24 2012 19:38:34 +01:00 ADMIN_DIR
6 -rwx  10303  Mar 15 2012 18:37:20 +01:00 startup-config.bak
7 -rwx   7366  Apr 20 2012 10:57:02 +01:00 startup-config
8 -rwx      4  Feb 19 2012 07:05:02 +01:00 dhcpBindConflict
9 -rwx  12829  Feb 18 2012 02:24:14 +01:00 startup-
config.backup
10 drwx  4096  Mar 08 2012 22:58:54 +01:00 WJ_running-config
11 -rwx  7689  Feb 21 2012 04:45:40 +01:00 stbkup

flash: 2143281152 bytes total (2131476480 bytes free)

Dell#
```

Example (Partial)

```
Dell#show tech-support stack-unit 0
Required Type : -

-- Unit 5 --
Unit Type     : Member Unit
Status        : not present
Required Type : -

------------------ show environment -------------------

-- Unit Environment Status --
Unit Status Temp Voltage
-----------------------------------------------------
* 1 online 41C ok

* Management Unit

-- Thermal Sensor Readings (deg C) --
Unit Sensor0 Sensor1
---------------------------
1    39       41

--------------------- show ip traffic -------------------
IP statistics:
  Rcvd: 894390 total, 415557 local destination
    0 format errors, 0 checksum errors, 0 bad hop count
    0 unknown protocol, 0 not a gateway
    15 security failures, 0 bad options
  Frags: 0 reassembled, 0 timeouts, 0 too big
    0 fragmented, 0 couldn't fragment
  Bcast: 402 received, 0 sent; Mcast: 37 received, 0 sent
  Sent: 468133 generated, 0 forwarded
    42 encapsulation failed, 0 no route
```

```
ICMP statistics:
  Rcvd: 0 format errors, 0 checksum errors, 0 redirects, 2
unreachable
    0 echo, 0 echo reply, 0 mask requests, 0 mask replies, 0
quench
    0 parameter, 0 timestamp, 0 info request, 0 other
  Sent: 0 redirects, 0 unreachable, 0 echo, 0 echo reply
    0 mask requests, 0 mask replies, 0 quench, 0 timestamp
    0 info reply, 0 time exceeded, 0 parameter problem

UDP statistics:
  Rcvd: 396516 total, 0 checksum errors, 0 no port
    0 short packets, 0 bad length, 28746 no port broadcasts, 0
socket full
  Sent: 16460 total, 28746 forwarded broadcasts

TCP statistics:
  Rcvd: 4618 total, 0 checksum errors, 0 no port
  Sent: 5023 total

ARP statistics:
  Rcvd: 43988 requests, 24518 replies, 10 wrong interface
  Sent: 42 requests, 6 replies (0 proxy)
```

Related Commands

show version — Displays the Dell Networking OS version.

show system — Displays the current switch status.

show environment — Displays the system component status.

show processes memory — Displays memory usage based on running processes.

telnet

Connect through Telnet to a server. The Telnet client and server in the Dell Networking Operating System (OS) support IPv4 connections. You can establish a Telnet session directly to the router or a connection can be initiated from the router.

Syntax `telnet {host | ip-address} [/source-interface]`

Parameters

host	Enter the name of a server.
ip-address	Enter the IPv4 address in dotted decimal format of the server.
source-interface	(OPTIONAL) Enter the keywords `/source-interface` then the interface information to include the source interface. Enter the following keywords and slot/port or number information: • For a Loopback interface, enter the keyword `loopback` then a number from zero (0) to 16383. • For the Null interface, enter the keyword `null` then 0.

- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

Defaults Not configured.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

terminal xml

Enable XML mode in Telnet and SSH client sessions.

Syntax `terminal xml`

To exit XML mode, use the `terminal no xml` command.

Defaults Disabled

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information This command enables the XML input mode where you can either cut and paste XML requests or enter the XML requests line-by-line. For more information about using the XML feature, refer to the XML chapter in the *Dell Networking OS Configuration Guide*.

traceroute

View a packet’s path to a specific device.

Syntax `traceroute {host | ip-address}`

Parameters

host	Enter the name of device.
ip-address	Enter the IP address of the device in dotted decimal format.

Defaults

- Timeout = **5 seconds**
- Probe count = **3**
- 30 hops max
- 40 byte packet size
- UDP port = **33434**

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

When you enter the `traceroute` command without specifying an IP address (Extended Traceroute), you are prompted for a target and source IP address, timeout (in seconds) (default is **5**), a probe count (default is **3**), minimum TTL (default is **1**), maximum TTL (default is **30**), and port number (default is **33434**). To keep the default setting for those parameters, press the ENTER key.

Example (IPv4)

```
Dell#traceroute www.force10networks.com

Translating "www.force10networks.com"...domain server
(10.11.0.1) [OK]
Type Ctrl-C to abort.

-----------------------------------------------
Tracing the route to www.force10networks.com (10.11.84.18),
30 hops max, 40 byte packets
-----------------------------------------------

TTL Hostname      Probe1     Probe2     Probe3
1   10.11.199.190 001.000 ms 001.000 ms 002.000 ms
2   gwegress-sjc-02.force10networks.com (10.11.30.126) 005.000
ms 001.000 ms 001.000 ms
3   fw-sjc-01.force10networks.com (10.11.127.254) 000.000 ms
000.000 ms 000.000 ms
4   www.force10networks.com (10.11.84.18) 000.000 ms 000.000
ms 000.000 ms
Dell#
```

Related Commands

ping — tests the connectivity to a device.

undebug all

Disable all debug operations on the system.

Syntax	`undebug all`
Defaults	none
Command Modes	EXEC Privilege
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

virtual-ip

Configure a virtual IP address for the active management interface. You can configure virtual addresses both for IPv4 independently.

Syntax	`virtual-ip {`*`ipv4-address`*`}`	
Parameters	*ipv4-address*	Enter the IP address of the active management interface in a dotted decimal format (A.B.C.D.).
Defaults	none	
Command Modes	CONFIGURATION	
Command History	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	Each time you issue this command, it replaces the previously configured address of the same family. The `no virtual-ip` command takes an address/prefix-length argument, so that the desired address only is removed. If you enter the `no virtual-ip` command without any specified address, the IPv4 virtual addresses are removed.	

Example

```
Dell#virtual-ip 10.11.197.99/16
```

write

Copy the current configuration to either the startup-configuration file or the terminal.

Syntax	`write {memory	terminal}`	
Parameters	memory	Enter the keyword `memory` to copy the current running configuration to the startup configuration file. This

	command is similar to the `copy running-config startup-config` command.
terminal	Enter the keyword `terminal` to copy the current running configuration to the terminal. This command is similar to the `show running-config` command.

Command Modes EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information The `write memory` command saves the running-configuration to the file labeled startup-configuration. When using a LOCAL CONFIG FILE other than the startup-config not named "startup-configuration," the running-config is not saved to that file; use the `copy` command to save any running-configuration changes to that local file.

5

802.1X

An authentication server must authenticate a client connected to an 802.1X switch port. Until the authentication, only extensible authentication protocol over LAN (EAPOL) traffic is allowed through the port to which a client is connected. After authentication is successful, normal traffic passes through the port.

The Dell Networking operating software supports remote authentication dial-in service (RADIUS) and active directory environments using 802.1X Port Authentication.

Important Points to Remember

The system limits network access for certain users by using virtual local area network (VLAN) assignments. 802.1X with VLAN assignment has these characteristics when configured on the switch and the RADIUS server.

- If no VLAN is supplied by the RADIUS server or if you disable 802.1X authorization, the port configures in its access VLAN after successful authentication.
- If you enable 802.1X authorization but the VLAN information from the RADIUS server is not valid, the port returns to the Unauthorized state and remains in the configured access VLAN. This safeguard prevents ports from appearing unexpectedly in an inappropriate VLAN due to a configuration error. Configuration errors create an entry in Syslog.
- If you enable 802.1X authorization and all information from the RADIUS server is valid, the port is placed in the specified VLAN after authentication.
- If you enable port security on an 802.1X port with VLAN assignment, the port is placed in the RADIUS server assigned VLAN.
- If you disable 802.1X on the port, it returns to the configured access VLAN.
- When the port is in the Force Authorized, Force Unauthorized, or Shutdown state, it is placed in the configured access VLAN.
- If an 802.1X port is authenticated and put in the RADIUS server assigned VLAN, any change to the port access VLAN configuration does not take effect.
- The 802.1X with VLAN assignment feature is not supported on trunk ports, dynamic ports, or with dynamic-access port assignment through a VLAN membership.

debug dot1x

Display 802.1X debugging information.

Syntax

```
debug dot1x [all | auth-pae-fsm | backend-fsm | eapol-pdu]
[interface interface]
```

Parameters

all	Enable all 802.1X debug messages.
auth-pae-fsm	Enable authentication PAE FSM debug messages.
backend-fsm	Enable backend FSM debug messages.
eapol-pdu	Enable the EAPOL frame trace and related debug messages.
interface *interface*	Restricts the debugging information to an interface.

Defaults Disabled

Command Modes EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

dot1x auth-fail-vlan

Configure an authentication failure VLAN for users and devices that fail 802.1X authentication.

Syntax `dot1x auth-fail-vlan vlan-id [max-attempts number]`

To delete the authentication failure VLAN, use the `no dot1x auth-fail-vlan vlan-id [max-attempts number]` command.

Parameters

vlan-id	Enter the VLAN Identifier. The range is from 1 to 4094.
max-attempts *number*	(OPTIONAL) Enter the keywords `max-attempts` followed number of attempts desired before authentication fails. The range is from 1 to 5. The default is **3**.

Defaults **3** attempts

Command Modes CONFIGURATION (*conf-if-interface-slot/port*)

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

If the host responds to 802.1X with an incorrect login/password, the login fails. The switch attempts to authenticate again until the maximum attempts configured is reached. If the authentication fails after all allowed attempts, the interface moves to the authentication failed VLAN.

After the authentication VLAN is assigned, the port-state must be toggled to restart authentication. Authentication occurs at the next reauthentication interval (`dot1x reauthentication`).

Related Commands	- dot1x port-control — Enables port control on an interface. - dot1x guest-vlan — Configures a guest VLAN for limited access users or for devices that are not 802.1X capable. - show dot1x interface — Displays the 802.1X configuration of an interface.

dot1x auth-server

Configure the authentication server to RADIUS.

Syntax	`dot1x auth-server radius`	
Defaults	none	
Command Modes	CONFIGURATION	
Command History	**Version 9.2(0.0)**	Introduced on the MXL 10/40GbE Switch IO Module.

dot1x auth-type mab-only

To authenticate a device with MAC authentication bypass (MAB), only use the host MAC address.

Syntax	`dot1x auth-type mab-only`	
Defaults	Disabled	
Command Modes	INTERFACE	
Command History	**Version 9.2(0.0)**	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The prerequisites for enabling MAB-only authentication on a port are:

- Enable 802.1X authentication globally on the switch and on the port (the `dot1x authentication` command).
- Enable MAC authentication bypass on the port (the `dot1x mac-auth-bypass` command).

In MAB-only authentication mode, a port authenticates using the host MAC address even though 802.1xauthentication is enabled. If the MAB-only authentication fails, the host is placed in the guest VLAN (if configured).

To disable MAB-only authentication on a port, enter the `no dot1x auth-type mab-only` command.

Related Commands	dot1x mac-auth-bypass — Enables MAC authentication bypass.

dot1x authentication (Configuration)

Enable dot1x globally. Enable dot1x both globally and at the interface level.

Syntax	`dot1x authentication` To disable dot1x on a globally, use the `no dot1x authentication` command.
Defaults	Disabled
Command Modes	CONFIGURATION
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	dot1x authentication (Interface) — Enables dot1x on an interface.

dot1x authentication (Interface)

Enable dot1x on an interface. Enable dot1x both globally and at the interface level.

Syntax	`dot1x authentication` To disable dot1x on an interface, use the `no dot1x authentication` command.
Defaults	Disabled
Command Modes	INTERFACE
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	dot1x authentication (Configuration) — Enable dot1x globally.

dot1x guest-vlan

Configure a guest VLAN for limited access users or for devices that are not 802.1X capable.

Syntax	`dot1x guest-vlan` *`vlan-id`*

To disable the guest VLAN, use the `no dot1x guest-vlan vlan-id` command.

Parameters

vlan-id	Enter the VLAN Identifier. The range is from 1 to 4094.

Defaults

Not configured.

Command Modes

CONFIGURATION (*conf-if-interface-slot/port*)

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

1X authentication is enabled when an interface is connected to the switch. If the host fails to respond within a designated amount of time, the authenticator places the port in the guest VLAN.

If a device does not respond within 30 seconds, it is assumed that the device is not 802.1X capable. Therefore, a guest VLAN is allocated to the interface and authentication, for the device, occurs at the next reauthentication interval (`dot1x reauthentication`).

If the host fails authentication for the designated number of times, the authenticator places the port in authentication failed VLAN (`dot1x auth-fail-vlan`).

NOTE: You can create the Layer 3 portion of a guest VLAN and authentication fail VLANs regardless if the VLAN is assigned to an interface or not. After an interface is assigned a guest VLAN (which has an IP address), routing through the guest VLAN is the same as any other traffic. However, the interface may join/leave a VLAN dynamically.

Related Commands

- dot1x auth-fail-vlan — Configures an authentication failure VLAN.
- dot1x reauthentication — Enables periodic re-authentication of the client.
- dot1x reauth-max — Configure the maximum number of times to re-authenticate a port before it becomes unauthorized.

dot1x host-mode

Enable single-host or multi-host authentication.

Syntax

```
dot1x host-mode {single-host | multi-host | multi-auth}
```

Parameters

single-host	Enable single-host authentication.
multi-host	Enable multi-host authentication.
multi-auth	Enable multi-supplicant authentication.

Defaults	**single-host**
Command Modes	INTERFACE
Command History	Version 9.2(0.0) — Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

- Single-host mode authenticates only one host per authenticator port and drops all other traffic on the port.
- Multi-host mode authenticates the first host to respond to an Identity Request and then permits all other traffic on the port.
- Multi-supplicant mode authenticates every device attempting to connect to the network on the authenticator port.

dot1x mac-auth-bypass

Enable MAC authentication bypass. If 802.1X times out because the host did not respond to the Identity Request frame, the system attempts to authenticate the host based on its MAC address.

Syntax

```
dot1x mac-auth-bypass
```

To disable MAC authentication bypass on a port, use the `no dot1x mac-auth-bypass` command.

Defaults	Disabled
Command Modes	INTERFACE
Command History	Version 9.2(0.0) — Introduced on the MXL 10/40GbE Switch IO Module.

dot1x max-eap-req

Configure the maximum number of times an extensive authentication protocol (EAP) request is transmitted before the session times out.

Syntax

```
dot1x max-eap-req number
```

To return to the default, use the `no dot1x max-eap-req` command.

Parameters

number	Enter the number of times an EAP request is transmitted before a session time-out. The range is from 1 to 10. The default is **2**.

Defaults	**2**
Command Modes	INTERFACE
Command History	Version 9.2(0.0) — Introduced on the MXL 10/40GbE Switch IO Module.

dot1x max-supplicants

Restrict the number of supplicants that can be authenticated and permitted to access the network through the port. This configuration is only takes effect in Multi-Auth mode.

Syntax

```
dot1x max-supplicants number
```

Parameters

number	Enter the number of supplicants that can be authenticated on a single port in Multi-Auth mode. The range is from 1 to 128. The default is **128**.

Defaults	128 hosts can be authenticated on a single authenticator port.
Command Modes	INTERFACE
Command History	Version 9.2(0.0) — Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	dot1x host-mode — Enables single-host or multi-host authentication.

dot1x port-control

Enable port control on an interface.

Syntax

```
dot1x port-control {force-authorized | auto | force-
unauthorized}
```

Parameters

force-authorized	Enter the keywords `force-authorized` to forcibly authorize a port.
auto	Enter the keyword `auto` to authorize a port based on the 802.1X operation result.
force-unauthorized	Enter the keywords `force-unauthorized` to forcibly deauthorize a port.

Defaults	none

Command Modes

Auto

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The authenticator completes authentication only when `port-control` is set to `auto`.

dot1x quiet-period

Set the number of seconds that the authenticator remains quiet after a failed authentication with a client.

Syntax

`dot1x quiet-period` *`seconds`*

To disable quiet time, use the `no dot1x quiet-time` command.

Parameters

seconds	Enter the number of seconds. The range is from 1 to 65535. The default is **60**.

Defaults

60 seconds

Command Modes

INTERFACE

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

dot1x reauthentication

Enable periodic reauthentication of the client.

Syntax

`dot1x reauthentication [interval` *`seconds`*`]`

To disable periodic reauthentication, use the `no dot1x reauthentication` command.

Parameters

interval *seconds*	(Optional) Enter the keyword `interval` then the interval time, in seconds, after which reauthentication is initiated. The range is from 1 to 31536000 (one year). The default is **3600** (1 hour).

Defaults

3600 seconds (1 hour)

Command Modes

INTERFACE

Command History	Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

dot1x reauth-max

Configure the maximum number of times a port can reauthenticate before the port becomes unauthorized.

Syntax

`dot1x reauth-max number`

To return to the default, use the `no dot1x reauth-max` command.

Parameters

number	Enter the permitted number of reauthentications. The range is from 1 to 10. The default is **2**.

Defaults **2**

Command Modes INTERFACE

Command History	Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

dot1x server-timeout

Configure the amount of time after which exchanges with the server time-out.

Syntax

`dot1x server-timeout seconds`

To return to the default, use the `no dot1x server-timeout` command.

Parameters

seconds	Enter a time-out value in seconds. The range is from 1 to 300, where 300 is implementation dependant. The default is **30**.

Defaults **30** seconds

Command Modes INTERFACE

Command History	Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

When you configure the `dot1x server-timeout` value, take into account the communication medium used to communicate with an authentication server and the number of RADIUS servers configured. Ideally, the `dot1x server-timeout` value (in seconds) is based on the configured RADIUS-server timeout and retransmit values and calculated according to the following formula: `dot1x server-timeout` *seconds* > (radius-server retransmit *seconds* + 1) * radius-server timeout *seconds*.

Where the default values are as follows: `dot1x server-timeout` (30 seconds), radius-server retransmit (3 seconds), and radius-server timeout (5 seconds).

For example:

```
Dell(conf)#radius-server host 10.11.197.105 timeout 6
Dell(conf)#radius-server host 10.11.197.105 retransmit 4
Dell(conf)#interface gigabitethernet 2/23
Dell(conf-if-gi-2/23)#dot1x server-timeout 40
```

dot1x supplicant-timeout

Configure the amount of time after which exchanges with the supplicant time-out.

Syntax

`dot1x supplicant-timeout` *`seconds`*

To return to the default, use the `no dot1x supplicant-timeout` command.

Parameters

seconds	Enter a time-out value in seconds. The range is from 1 to 300, where 300 is implementation dependant. The default is **30**.

Defaults

30 seconds

Command Modes

INTERFACE

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

dot1x tx-period

Configure the intervals at which EAPOL PDUs the Authenticator PAE transmits.

Syntax

`dot1x tx-period` *`seconds`*

To return to the default, use the `no dot1x tx-period` command.

Parameters

seconds	Enter the interval time, in seconds, that EAPOL PDUs are transmitted. The range is from 1 to 65535. The default is **30**.

Defaults	**30** seconds
Command Modes	INTERFACE
Command History	Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

show dot1x cos-mapping interface

Display the CoS priority-mapping table the RADIUS server provides and applies to authenticated supplicants on an 802.1X-enabled system.

Syntax

`show dot1x cos-mapping interface` *`interface`* `[mac-address` *`mac-address`*`]`

Parameters

interface	Enter one of the following keywords and slot/port or number information: • For a Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the slot/port information. • For a Fast Ethernet interface, enter the keyword `FastEthernet` then the slot/port information. • For a Ten-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
mac-address	(Optional) MAC address of an 802.1X-authenticated supplicant.

Defaults

none

Command Modes

- EXEC
- EXEC privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To display CoS mapping information only for the specified supplicant, enter a supplicant's MAC address using the `mac-address` option.

You can display the CoS mapping information applied to traffic from authenticated supplicants on 802.1X-enabled ports that are in Single-Hot, Multi-Host, and Multi-Supplicant authentication modes.

Example

```
Dell#show dot1x cos-mapping interface tengigabitethernet 0/32

802.1p CoS re-map table on Te 0/32:
----------------------------------
Dot1p        Remapped Dot1p
```

```
0           7
1           6
2           5
3           4
4           3
5           2
6           1
7           0
Dell#

Dell#show dot1x cos-mapping interface tengigabitethernet 0/32
mac-address 00:00:00:00:00:10
Supplicant Mac: 0 0 0 0 0 10 Lookup for Mac:

802.1p CoS re-map table on Te 0/32:
----------------------------------

802.1p CoS re-map table for Supplicant: 00:00:00:00:00:10

Dot1p        Remapped Dot1p
0            7
1            6
2            5
3            4
4            3
5            2
6            1
7            0
Dell#
```

show dot1x interface

Display the 802.1X configuration of an interface.

Syntax `show dot1x interface` *`interface`* `[mac-address` *`mac-address`*`]`

Parameters

interface	Enter one of the following keywords and slot/port or number information: • For a Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the slot/port information. • For a Fast Ethernet interface, enter the keyword `FastEthernet` then the slot/port information. • For a Ten-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
mac-address	(Optional) MAC address of a supplicant.

Defaults none

Command Modes

- EXEC
- EXEC privilege

Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

If you enable 802.1X multi-supplicant authentication on a port, additional 802.1X configuration details (Port Authentication status, Untagged VLAN ID, Authentication PAE state, and Backend state) are displayed for each supplicant, as shown in the following example.

Example

```
Dell#show dot1x interface fortyGigE 0/48

802.1x information on Fo 0/48:
-----------------------------
Dot1x Status:             Enable
Port Control:             AUTO
Port Auth Status:         UNAUTHORIZED
Re-Authentication:        Disable
Untagged VLAN id:         None
Guest VLAN:               Disable
Guest VLAN id:            NONE
Auth-Fail VLAN:           Disable
Auth-Fail VLAN id:        NONE
Auth-Fail Max-Attempts:   NONE
Mac-Auth-Bypass:          Disable
Mac-Auth-Bypass Only:     Disable
Tx Period:                30 seconds
Quiet Period:             60 seconds
ReAuth Max:               2
Supplicant Timeout:       30 seconds
Server Timeout:           30 seconds
Re-Auth Interval:         3600 seconds
Max-EAP-Req:              2
Host Mode:                SINGLE_HOST
Auth PAE State:           Initialize
Backend State:            Initialize
Dell#

Dell#show dot1x interface tengigabitethernet 0/32

802.1x information on Te 0/32:
-----------------------------
Dot1x Status:             Enable
Port Control:             AUTO
Port Auth Status:         AUTHORIZED(MAC-AUTH-BYPASS)
Re-Authentication:        Disable
Untagged VLAN id:         400
Guest VLAN:               Enable
Guest VLAN id:            100
Auth-Fail VLAN:           Disable
Auth-Fail VLAN id:        NONE
Auth-Fail Max-Attempts:   NONE
Mac-Auth-Bypass:          Enable
Mac-Auth-Bypass Only:     Enable
Tx Period:                3 seconds
Quiet Period:             60 seconds
ReAuth Max:               2
Supplicant Timeout:       30 seconds
Server Timeout:           30 seconds
Re-Auth Interval:         3600 seconds
Max-EAP-Req:              2
Host Mode:                SINGLE_HOST
Auth PAE State:           Authenticated
```

```
Backend State:            Idle
Dell#

Dell#show dot1x interface tengigabitethernet 0/32 mac-address
00:00:00:00:00:10
Supplicant Mac: 0 0 0 0 0 10 Lookup for Mac:

802.1x information on Te 0/32:
-----------------------------
Dot1x Status:             Enable
Port Control:             AUTO
Re-Authentication:        Disable
Guest VLAN:               Enable
Guest VLAN id:            100
Auth-Fail VLAN:           Disable
Auth-Fail VLAN id:        NONE
Auth-Fail Max-Attempts:   NONE
Mac-Auth-Bypass:          Enable
Mac-Auth-Bypass Only:     Enable
Tx Period:                3 seconds
Quiet Period:             60 seconds
ReAuth Max:               2
Supplicant Timeout:       30 seconds
Server Timeout:           30 seconds
Re-Auth Interval:         3600 seconds
Max-EAP-Req:              2
Host Mode:                MULTI_AUTH
Max-Supplicants:          128

Port status and State info for Supplicant: 00:00:00:00:00:10

Port Auth Status:         AUTHORIZED(MAC-AUTH-BYPASS)
Untagged VLAN id:         400
Auth PAE State:           Authenticated
Backend State:            Idle
Dell#
```

Example (mac-address)

```
Dell#show dot1x interface gig 2/21 mac-address
00:00:01:00:07:00

802.1x information on Gi 2/21:
-----------------------------
Dot1x Status:           Enable
Port Control:           AUTO
Re-Authentication:      Disable
Guest VLAN:             Disable
Guest VLAN id:          NONE
Auth-Fail VLAN:         Disable
Auth-Fail VLAN id:      NONE
Auth-Fail Max-Attempts: NONE
Mac-Auth-Bypass:        Enable
Mac-Auth-Bypass Only:   Disable
Tx Period:              5 seconds
Quiet Period:           60 seconds
ReAuth Max:             1
Supplicant Timeout:     30 seconds
Server Timeout:         30 seconds
Re-Auth Interval:       60 seconds
Max-EAP-Req:            2
Host Mode:              MULTI_AUTH
Max-Supplicants:        128

Port status and State info for Supplicant: 00:00:01:00:07:00
Port Auth Status:       AUTHORIZED(MAC-AUTH-BYPASS)
Untagged VLAN id:       4094
Auth PAE State:         Authenticated
Backend State:          Idle
Dell#
```

Example (Interface)

```
Dell#show dot1x interface g 0/21

802.1x information on Gi 0/21:
-----------------------------
Dot1x Status:           Enable
Port Control:           AUTO
Re-Authentication:      Disable
Guest VLAN:             Enable
Guest VLAN id:          100
Auth-Fail VLAN:         Disable
Auth-Fail VLAN id:      NONE
Auth-Fail Max-Attempts: NONE
Mac-Auth-Bypass:        Disable
Mac-Auth-Bypass Only:   Disable
Tx Period:              30 seconds
Quiet Period:           60 seconds
ReAuth Max:             3
Supplicant Timeout:     30 seconds
Server Timeout:         30 seconds
Re-Auth Interval:       60 seconds
Max-EAP-Req:            2
Host Mode:              MULTI_AUTH
Max-Supplicants:        128

Port status and State info for Supplicant: 00:00:00:00:00:10

Port Auth Status:       AUTHORIZED
Untagged VLAN id:       400
Auth PAE State:         Authenticated
Backend State:          Idle

Port status and State info for Supplicant: 00:00:00:00:00:11
192 | 802.1X
www.dell.com | s u p p o r t . d e l l.com
Port Auth Status:       AUTHORIZED
Untagged VLAN id:       300
Auth PAE State:         Authenticated
Backend State:          Idle

Port status and State info for Supplicant: 00:00:00:00:00:15

Port Auth Status:       AUTHORIZED(GUEST-VLAN)
Untagged VLAN id:       100
Auth PAE State:         Authenticated
Backend State:          Idle
```

6

Access Control Lists (ACL)

Access control lists (ACLs) are supported by the Dell Networking Operating System (OS).

The Dell Networking OS supports the following types of ACL, IP prefix list, and route maps:

- Commands Common to all ACL Types
- Common IP ACL Commands
- Standard IP ACL Commands
- Extended IP ACL Commands
- Common MAC Access List Commands
- Standard MAC ACL Commands
- Extended MAC ACL Commands
- IP Prefix List Commands
- Route Map Commands

NOTE: For ACL commands that use the Trace function, refer to the Secure DHCP Commands section in the Security chapter.

Commands Common to all ACL Types

The following commands are available within each ACL mode and do not have mode-specific options. Some commands in this chapter may use similar names, but require different options to support the different ACL types (for example, the `deny` command).

description

Configure a short text string describing the ACL.

Syntax	`description` *`text`*
Parameters	*text* Enter a text string up to 80 characters long.
Defaults	Not enabled.
Command Modes	• CONFIGURATION-IP ACCESS-LIST-STANDARD • CONFIGURATION-IP ACCESS-LIST-EXTENDED • CONFIGURATION-MAC ACCESS LIST-STANDARD • CONFIGURATION-MAC ACCESS LIST-EXTENDED

Command History		
	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

remark

Enter a description for an ACL entry.

Syntax `remark [remark-number] [description]`

Parameters

remark-number	Enter the remark number. The range is from 0 to 4294967290. **NOTE:** You can use the same sequence number for the remark and an ACL rule.
description	Enter a description of up to 80 characters.

Defaults Not configured.

Command Modes

- CONFIGURATION-IP ACCESS-LIST-STANDARD
- CONFIGURATION-IP ACCESS-LIST-EXTENDED
- CONFIGURATION-MAC ACCESS LIST-STANDARD
- CONFIGURATION-MAC ACCESS LIST-EXTENDED

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The `remark` command is available in each ACL mode. You can configure up to 4294967290 remarks in a given ACL.

The following example shows the use of the `remark` command twice within CONFIGURATION-STANDARD-ACCESS-LIST mode. The same sequence number was used for the remark and for an associated ACL rule. The remark precedes the rule in the running-config because it is assumed that the remark is for the rule with the same sequence number, or the group of rules that follow the remark.

Example

```
Dell(conf-std-nacl)#remark 10 Deny rest of the traffic
Dell(conf-std-nacl)#remark 5 Permit traffic from XYZ Inc.
Dell(conf-std-nacl)#show config
!
ip access-list standard test
remark 5 Permit traffic from XYZ Inc.
seq 5 permit 1.1.1.0/24
remark 10 Deny rest of the traffic
seq 10 Deny any
Dell(conf-std-nacl)#
```

Related Commands

resequence access-list — Re-assigns sequence numbers to entries of an existing access-list.

resequence access-list

Re-assign sequence numbers to entries of an existing access-list.

Syntax

```
resequence access-list {ipv4 | mac} {access-list-name
StartingSeqNum Step-to-Increment}
```

Parameters

ipv4 | mac	Enter the keyword `ipv4` or `mac` to identify the access list type to resequence.
access-list-name	Enter the name of a configured IP access list.
StartingSeqNum	Enter the starting sequence number to resequence. The range is from 0 to 4294967290.
Step-to-Increment	Enter the step to increment the sequence number. The range is from 1 to 4294967290.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

When you have exhausted all the sequence numbers, this feature permits re-assigning a new sequence number to entries of an existing access-list.

Related Commands

resequence prefix-list ipv4 — resequences a prefix list.

resequence prefix-list ipv4

Re-assign sequence numbers to entries of an existing prefix list.

Syntax

```
resequence prefix-list ipv4 {prefix-list-name StartingSeqNum
Step-to-increment}
```

Parameters

prefix-list-name	Enter the name of the configured prefix list, up to 140 characters long.
StartingSeqNum	Enter the starting sequence number to resequence. The range is from 0 to 65535.
Step-to-Increment	Enter the step to increment the sequence number. The range is from 1 to 65535.

Defaults	none
Command Modes	- EXEC - EXEC Privilege
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	When you have exhausted all the sequence numbers, this feature permits re-assigning a new sequence number to entries of an existing prefix list.
Related Commands	seq — Assigns a sequence number to a deny or permit filter in an IP access list while creating the filter.

show config

Display the current ACL configuration.

Syntax	`show config`
Command Modes	- CONFIGURATION-IP ACCESS-LIST-STANDARD - CONFIGURATION-IP ACCESS-LIST-EXTENDED - CONFIGURATION-MAC ACCESS LIST-STANDARD - CONFIGURATION-MAC ACCESS LIST-EXTENDED
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell(config-std-nacl)#show conf
!
ip access-list standard test
remark 5 Permit traffic from XYZ Inc.
seq 5 permit 1.1.1.0/24 count
remark 10 Deny traffic from ABC
seq 10 deny 2.1.1.0/24 count
Dell(config-std-nacl)#
```

Common IP ACL Commands

The following commands are available within both IP ACL modes (Standard and Extended) and do not have mode-specific options. When an ACL is created without a rule and then is applied to an interface, ACL behavior reflects an implicit permit.

The MXL 10/40GbE Switch IO Module platform supports both Ingress and Egress IP ACLs.

NOTE: Also refer to the Commands Common to all ACL Types section.

access-class

Apply a standard ACL to a terminal line.

Syntax	`access-class` *`access-list-name`*
Parameters	*access-list-name*: Enter the name of a configured Standard ACL, up to 140 characters.
Defaults	Not configured.
Command Modes	LINE
Command History	Version 8.3.16.1: Introduced on the MXL 10/40GbE Switch IO Module.

clear counters ip access-group

Erase all counters maintained for access lists.

Syntax	`clear counters ip access-group [`*`access-list-name`*`]`
Parameters	*access-list-name*: (OPTIONAL) Enter the name of a configured access-list, up to 140 characters.
Command Modes	EXEC Privilege
Command History	Version 8.3.16.1: Introduced on the MXL 10/40GbE Switch IO Module.

ip access-group

Apply an egress IP ACL to an interface.

Syntax	`ip access-group` *`access-list-name`* `{in	out} [implicit-permit] [vlan` *`vlan-id`*`]`
Parameters	access-list-name: Enter the name of a configured access list, up to 140 characters.

in	Enter the keyword `in` to apply the ACL to incoming traffic.
out	Enter the keyword `out` to apply the ACL to the outgoing traffic.
implicit-permit	(OPTIONAL) Enter the keyword `implicit-permit` to change the default action of the ACL from implicit-deny to implicit-permit (that is, if the traffic does not match the filters in the ACL, the traffic is permitted instead of dropped).
vlan *vlan-id*	(OPTIONAL) Enter the keyword `vlan` then the ID numbers of the VLANs.

Defaults Not enabled..

Command Modes INTERFACE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module platform.

Usage Information

You can assign one ACL (standard or extended ACL) to an interface..

NOTE: This command is *not* supported on the MXL Switch Loopback interfaces.

When you apply an ACL that filters IGMP traffic, all IGMP traffic is redirected to the CPUs and soft-forwarded, if necessary, in the following scenarios:

- on a Layer 2 interface — if a Layer 3 ACL is applied to the interface
- on a Layer 3 port or on a Layer 2/Layer 3 port

Related Commands

ip access-list standard — configures a standard ACL.

ip access-list extended — configures an extended ACL.

show ip access-lists

Display all of the IP ACLs configured in the system, whether or not they are applied to an interface, and the count of matches/mismatches against each ACL entry displayed.

Syntax

```
show ip access-lists [access-list-name] [interface interface]
[in]
```

Parameters

access-list-name	Enter the name of a configured MAC ACL, up to 140 characters.
interface *interface*	Enter the keyword `interface` then the one of the following keywords and slot/port or number information:

	• For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
in	Identify whether ACL is applied on the ingress or egress side.

Command Modes: EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show ip access-lists  test  in
Standard Ingress IP access list test
seq 5 permit 1.1.1.0/24 count (0 packets)
seq 10 deny 2.1.1.0/24 count (0 packets)
```

show ip accounting access-list

Display the IP access-lists created on the switch and the sequence of filters.

Syntax

```
show ip accounting {access-list access-list-name | cam_count}
interface interface
```

Parameters

access-list-name	Enter the name of the ACL to be displayed.
cam_count	List the count of the CAM rules for this ACL.
interface *interface*	Enter the keyword `interface` then the one of the following keywords and slot/port or number information: • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

show ip accounting access-lists Field	Description
"Extended IP..."	Displays the name of the IP ACL.
"seq 5..."	Displays the filter. If the keywords `count` or `byte` were configured in the filter, the number of packets or bytes the filter processes is displayed at the end of the line.
"order 4"	Displays the QoS order of priority for the ACL entry.

Example

```
Dell#show ip accounting access-list
!
Standard Ingress IP access list test on TenGigabitEthernet 0/88
Total cam count 2
seq 5 permit 1.1.1.0/24 count (0 packets)
seq 10 deny 2.1.1.0/24 count (0 packets)
```

Standard IP ACL Commands

When you create an ACL without any rule and then apply it to an interface, the ACL behavior reflects an implicit permit.

The MXL 10/40GbE Switch IO Module platform supports both Ingress and Egress IP ACLs.

NOTE: Also refer to the Commands Common to all ACL Types and Common IP ACL Commands sections.

deny (for Standard IP ACLs)

To drop packets with a certain IP address, configure a filter.

Syntax

`deny {source | any | host {ip-address}}[count [byte]] [dscp value] [order] [fragments] [log [interval minutes] [threshold-in-msgs [count]] [monitor]`

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no deny {source [mask] | any | host ip-address}` command.

Parameters

source	Enter the IP address of the network or host from which the packets were sent.

any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword `host` then the IP address to specify a host IP address.
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.
dscp	Enter this keyword `dscp` to deny a packet based on the DSCP value. The range is from 0 to 63.
log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
order	(OPTIONAL) Enter the keyword `order` to specify the QoS priority for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority) If you did not use the keyword order, the ACLs have the lowest order by default (255).
fragments	Enter the keyword `fragments` to use ACLs to control packet fragments.
threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly.

The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

CONFIGURATION-STANDARD-ACCESS-LIST

Command History

Version 9.4(0.0)	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platforms.
Version 9.3(0.0)	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module platforms.

Usage Information	When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval. If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces. You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).
Related Commands	ip access-list standard — configures a standard ACL. permit — configures a permit filter.

ip access-list standard

Create a standard IP access list (IP ACL) to filter based on IP address.

Syntax	`ip access-list standard` *`access-list-name`*
Parameters	***access-list-name*** Enter a string up to 140 characters long as the ACL name.
Defaults	All IP access lists contain an implicit *deny any*, that is, if no match occurs, the packet is dropped.
Command Modes	CONFIGURATION
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information	The Dell operating system supports one ingress and one egress IP ACL per interface. The number of entries allowed per ACL is hardware-dependent. For detailed specifications on entries allowed per ACL, refer to your line card documentation.

Example

```
Dell(conf)#ip access-list standard TestList
Dell(config-std-nacl)#
```

Related Commands	ip access-list extended — creates an extended access list. resequence access-list — Displays the current configuration.

permit (for Standard IP ACLs)

To permit packets from a specific source IP address to leave the switch, configure a filter.

Syntax

```
permit {source [mask]| any | host ip-address} [count [byte]]
[dscp value] [order] [fragments] [log [interval minutes]
[threshold-in-msgs [count]] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq` *`sequence-number`* command if you know the filter's sequence number.
- Use the `no permit {`*`source`*` [`*`mask`*`] | any | host `*`ip-address`*`}` command.

Parameters

source	Enter the IP address in dotted decimal format of the network from which the packet was sent.
mask	(OPTIONAL) Enter a network `mask` in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword `host` then the IP address to specify a host IP address or hostname.
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
bytes	(OPTIONAL) Enter the keyword `bytes` to count bytes processed by the filter.
dscp	(OPTIONAL) Enter the keyword `dcsp` to match to the IP DCSCP values.

order	(OPTIONAL) Enter the keyword `order` to specify the QoS priority for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). If you do not use the keyword `order`, the ACLs have the lowest order by default (**255**).
fragments	Enter the keyword `fragments` to use ACLs to control packet fragments.
log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly.

The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

CONFIGURATION-STANDARD-ACCESS-LIST

Command History

Version 9.4(0.0)	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platforms.
Version 9.3(0.0)	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module platforms.

Usage Information

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

Related Commands

deny — assigns a IP ACL filter to deny IP packets.

ip access-list standard — creates a standard ACL.

seq

Assign a sequence number to a deny or permit filter in an extended IP access list while creating the filter.

Syntax

```
seq sequence-number {deny | permit} {source [mask] | any | host
ip-address}} [count [byte] [dscp value] [order] [fragments]
[log [interval minutes] [threshold-in-msgs [count] [monitor]
```

Parameters

sequence-number	Enter a number from 0 to 4294967290. The range is from 0 to 65534.
deny	Enter the keyword `deny` to configure a filter to drop packets meeting this condition.
permit	Enter the keyword `permit` to configure a filter to forward packets meeting this criteria.
source	Enter an IP address in dotted decimal format of the network from which the packet was received.
mask	(OPTIONAL) Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword `any` to specify that all routes are subject to the filter.
count	(OPTIONAL) Enter the keyword `count` to count packets the filter processes.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes the filter processes.
dscp	(OPTIONAL) Enter the keyword `dcsp` to match to the IP DCSCP values.

order	(OPTIONAL) Enter the keyword `order` to specify the QoS order for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). If you do not use the keyword `order`, the ACLs have the lowest order by default (**255**).
fragments	Enter the keyword `fragments` to use ACLs to control packet fragments.
log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
threshold-in *msgs* count	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` then by the time period in minutes at which the ACL logs must be generated. The interval range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

CONFIGURATION-IP ACCESS-LIST-STANDARD

Command History

Version 9.4(0.0)	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform.
Version 9.3(0.0)	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The `order` option is relevant in the context of the Policy QoS feature only. The following applies:

- The `seq` *`sequence-number`* command is applicable only in an ACL group.
- The `order` option works across ACL groups that have been applied on an interface via the QoS policy framework.
- The `order` option takes precedence over `seq` *`sequence-number`*.
- If *`sequence-number`* is not configured, the rules with the same order value are ordered according to their configuration order.

- If *`sequence-number`* is configured, the sequence-number is used as a tie breaker for rules with the same order.

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

Related Commands

deny — configures a filter to drop packets.

permit — configures a filter to forward packets.

seq — assigns a sequence number to a deny or permit filter in an IP access list while creating the filter.

Extended IP ACL Commands

When an ACL is created without any rule and then applied to an interface, ACL behavior reflects an implicit permit.

The following commands configure extended IP ACLs, which in addition to the IP address, also examine the packet’s protocol type.

The MXL 10/40GbE Switch IO Module platform supports both Ingress and Egress IP ACLs.

NOTE: Also refer to theCommands Common to all ACL Types and Common IP ACL Commands sections.

deny (for Extended IP ACLs)

Configure a filter that drops IP packets meeting the filter criteria.

Syntax

```
deny {ip | ip-protocol-number} {source mask | any | host ip-address}
{destination mask | any | host ip-address} [count
[byte]] [dscp value] [order] [monitor] [fragments] [log
[interval minutes] [threshold-in-msgs [count]] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter’s sequence number.
- Use the `no deny {ip | ip-protocol-number} {source mask | any | host ip-address} {destination mask | any | host ip-address}` command.

Parameters

source	Enter the IP address of the network or host from which the packets were sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword `host` then the IP address to specify a host IP address.
destination	Enter the IP address of the network or host to which the packets are sent.
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.
order	(OPTIONAL) Enter the keyword `order` to specify the QoS priority for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority) If you did not use the keyword `order`, the ACLs have the lowest order by default (255).
monitor	OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.
fragments	Enter the keyword `fragments` to use ACLs to control packet fragments.
log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.

threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The time interval range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly.

The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

CONFIGURATION-EXTENDED-ACCESS-LIST

Command History

Version 9.4(0.0)	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform.
Version 9.3(0.0)	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.

Usage Information

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

Related Commands	
	deny tcp — assigns a filter to deny TCP packets.
	deny udp — assigns a filter to deny UDP packets.
	ip access-list extended — creates an extended ACL.

deny icmp

To drop all or specific internet control message protocol (ICMP) messages, configure a filter.

Syntax

```
deny icmp {source mask | any | host ip-address} {destination
mask | any | host ip-address} [dscp] [count [byte]] [order]
[fragments][log interval minutes] [threshold-in-msgs] [count]]
[monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command, if you know the filter's sequence number.
- Use the `no deny icmp {source mask | any | host ip-address} {destination mask | any | host ip-address}` command.

Parameters

source	Enter the IP address of the network or host from which the packets were sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword `host` then the IP address to specify a host IP address.
destination	Enter the IP address of the network or host to which the packets are sent.
dscp	Enter this keyword `dscp` to deny a packet based on the DSCP value. The range is from 0 to 63.
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.
order	(OPTIONAL) Enter the keyword `order` to specify the QoS priority for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority) If you did not use the

	keyword `order`, the ACLs have the lowest order by default (255).
fragments	Enter the keyword `fragments` to use ACLs to control packet fragments.
log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
threshold-in *msgs count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The time interval range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

CONFIGURATION-IP ACCESS-LIST-EXTENDED

Command History

Version 9.4(0.0)	Added the support for flow-based monitoring on the MXL 10/40GbE Switch IO Module.
Version 9.3(0.0)	Added the support for logging ACLs on the MXL 10/40GbE Switch IO Module.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The `order` option is relevant in the context of the Policy QoS feature only. For more information, refer to the Quality of Service chapter of the *Dell Networking OS Configuration Guide*.

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure

ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable`command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

deny tcp

Configure a filter that drops transmission control protocol (TCP) packets meeting the filter criteria.

Syntax

```
deny tcp {source mask | any | host ip-address} [bit] [operator
port [port]] {destination mask | any | host ip-address} [dscp]
[bit] [operator port [port]] [count [byte] [order] [fragments]
[log [interval minutes] [threshold-in-msgs [count]] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq` *`sequence-number`* command if you know the filter's sequence number.
- Use the `no deny tcp {`*`source mask`*` | any | host `*`ip-address`*`} {`*`destination mask`*` | any | host `*`ip-address`*`}` command.

Parameters

source	Enter the IP address of the network or host from which the packets are sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword `host` then the IP address to specify a host IP address.
dscp	Enter this keyword `dscp` to deny a packet based on the DSCP value. The range is from 0 to 63.
bit	Enter a flag or combination of bits: • `ack:` acknowledgement field

	• `fin:` finish (no more data from the user) • `psh:` push function • `rst:` reset the connection • `syn:` synchronize sequence numbers • `urg:` urgent field
operator	(OPTIONAL) Enter one of the following logical operand: • `eq` = equal to • `neq` = not equal to • `gt` = greater than • `lt` = less than • `range` = inclusive range of ports (you must specify two ports for the `port` command)
port port	Enter the application layer port number. Enter two port numbers if using the range logical operand. The range is from 0 to 65535. The following list includes some common TCP port numbers: • 23 = Telnet • 20 and 21 = FTP • 25 = SMTP • 169 = SNMP
destination	Enter the IP address of the network or host to which the packets are sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
count	(OPTIONAL) Enter the keyword `count` to count packets the filter processes.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes the filter processes.
order	(OPTIONAL) Enter the keyword `order` to specify the QoS priority for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority) If you did not use the keyword `order`, the ACLs have the lowest order by default (**255**).
fragments	Enter the keyword `fragments` to use ACLs to control packet fragments.
log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.

threshold-in-msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly.

The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

CONFIGURATION-IP ACCESS-LIST-EXTENDED

Command History

9.4(0.0)	Added the support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platforms.
9.3(0.0)	Added the support for logging of ACLs on the MXL 10/40GbE Switch IO Module platforms.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The `order` option is relevant in the context of the Policy QoS feature only. For more information, refer to the Quality of Service chapter of the *Dell Networking OS Configuration Guide*.

In the MXL switch, you can configure either count (packets) or count (bytes). However, for an ACL with multiple rules, you can configure some ACLs with count (packets) and others as count (bytes) at any given time.

Most ACL rules require one entry in the CAM. However, rules with TCP and UDP port operators (for example, gt, lt, or range) may require more than one entry. The range of ports is configured in the CAM based on bit mask boundaries; the space required depends on exactly what ports are included in the range.

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

Example

An ACL rule with a TCP port range of 4000–8000 uses eight entries in the CAM.

```
Dell#  Data              Mask             From To #Covered

1 0000111110100000 1111111111100000 4000 4031 32
2 0000111111000000 1111111111000000 4032 4095 64
3 0001000000000000 1111100000000000 4096 6143 2048
4 0001100000000000 1111110000000000 6144 7167 1024
5 0001110000000000 1111111000000000 7168 7679 512
6 0001111000000000 1111111100000000 7680 7935 256
7 0001111100000000 1111111111000000 7936 7999 64
8 0001111101000000 1111111111111111 8000 8000 1

Total Ports: 4001
```

Example

An ACL rule with a TCP port lt 1023 uses only one entry in the CAM.

```
Dell# Data               Mask             From To   #Covered

1 0000000000000000 1111110000000000 0    1023 1024

Total Ports: 1024
```

Related Commands

deny — assigns a filter to deny IP traffic.

deny udp — assigns a filter to deny UDP traffic.

deny udp

To drop user datagram protocol (UDP) packets meeting the filter criteria, configure a filter.

Syntax

```
deny udp {source mask | any | host ip-address} [operator port
[port]] {destination mask | any | host ip-address} [dscp]
[operator port [port]] [count [byte]] [order] [fragments][log
[interval minutes] [threshold-in-msgs [count]]
```

To remove this filter, you have two choices:

- Use the `no seq` *`sequence-number`* command if you know the filter's sequence number.
- Use the `no deny udp {`*`source mask`*` | any | host `*`ip-address`*`} {`*`destination mask`*` | any | host `*`ip-address`*`}` command.

Parameters

source	Enter the IP address of the network or host from which the packets were sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword `host` then the IP address to specify a host IP address.
dscp	Enter this keyword `dscp` to deny a packet based on the DSCP value. The range is from 0 to 63.
operator	(OPTIONAL) Enter one of the following logical operand: • `eq` = equal to • `neq` = not equal to • `gt` = greater than • `lt` = less than • `range` = inclusive range of ports (you must specify two ports for the `port` command)
port port	Enter the application layer port number. Enter two port numbers if using the range logical operand. The range is from 0 to 65535.
destination	Enter the IP address of the network or host to which the packets are sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.
order	(OPTIONAL) Enter the keyword `order` to specify the QoS priority for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority) If you did not use the

	keyword `order`, the ACLs have the lowest order by default (**255**).
fragments	Enter the keyword `fragments` to use ACLs to control packet fragments.
log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
threshold-in-msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword then a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs are terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` then the time period in minutes at which the ACL logs must be generated. The time interval range is from 1 to 10 minutes.

Defaults

By default 10 ACL logs are generated if you do not specify the threshold explicitly.

The default frequency at which the ACL logs are generated is five minutes.

Command Modes

CONFIGURATION-IP ACCESS-LIST-EXTENDED

Command History

Version 9.3(0.0)	Added the support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The `order` option is relevant in the context of the Policy QoS feature only. For more information, refer to the Quality of Service chapter of the *Dell Networking OS Configuration Guide*.

In the MXL switch, you can configure either count (packets) or count (bytes). However, for an ACL with multiple rules, you can configure some ACLs with count (packets) and others as count (bytes) at any given time.

Most ACL rules require one entry in the CAM. However, rules with TCP and UDP port operators (for example, gt, lt or range) may require more than one entry. The range of ports is configured in the CAM based on bit mask boundaries; the space required depends on exactly what ports are included in the range.

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure

ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces

Example

An ACL rule with a TCP port range of 4000–8000 uses eight entries in the CAM.

```
Dell#  Data             Mask        From To #Covered

1 0000111110100000 1111111111100000 4000 4031 32
2 0000111111000000 1111111111000000 4032 4095 64
3 0001000000000000 1111100000000000 4096 6143 2048
4 0001100000000000 1111110000000000 6144 7167 1024
5 0001110000000000 1111111000000000 7168 7679 512
6 0001111000000000 1111111100000000 7680 7935 256
7 0001111100000000 1111111111000000 7936 7999 64
8 0001111101000000 1111111111111111 8000 8000 1

Total Ports: 4001
```

Example

An ACL rule with a TCP port lt 1023 uses only one entry in the CAM.

```
Dell# Data              Mask        From To   #Covered

1 0000000000000000 1111110000000000 0    1023 1024

Total Ports: 1024
```

Related Commands

deny — assigns a filter to deny IP traffic.

deny tcp — assigns a filter to deny TCP traffic.

ip access-list extended

Name (or select) an extended IP access list (IP ACL) based on IP addresses or protocols.

Syntax

`ip access-list extended` *`access-list-name`*

To delete an access list, use the `no ip access-list extended` *`access-list-name`* command.

Parameters

access-list-name	Enter a string up to 140 characters long as the access list name.

Defaults

All access lists contain an implicit *deny any*; that is, if no match occurs, the packet is dropped.

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The number of entries allowed per ACL is hardware-dependent. For detailed specification on entries allowed per ACL, refer to your line card documentation.

Example

```
Dell(conf)#ip access-list extended TESTListEXTEND
Dell(config-ext-nacl)#
```

Related Commands

ip access-list standard — configures a standard IP access list.

resequence access-list — Displays the current configuration.

permit (for Extended IP ACLs)

To pass IP packets meeting the filter criteria, configure a filter.

Syntax

`permit {source mask | any | host ip-address} {destination mask | any | host ip-address} [count [bytes]] [dscp value] [order] [fragments] [log [interval minutes] [threshold-in-msgs [count]] [monitor]`

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no deny {source mask | any | host ip-address} {destination mask | any | host ip-address}` command.

Parameters

source	Enter the IP address in dotted decimal format of the network from which the packet was sent.
mask	(OPTIONAL) Enter a network `mask` in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword `host` then the IP address to specify a host IP address or hostname.
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
bytes	(OPTIONAL) Enter the keyword `bytes` to count bytes processed by the filter.
dscp	(OPTIONAL) Enter the keyword `dcsp` to match to the IP DCSCP values.
order	(OPTIONAL) Enter the keyword order to specify the QoS priority for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). If you do not use the

	keyword `order`, the ACLs have the lowest order by default (**255**).
fragments	Enter the keyword `fragments` to use ACLs to control packet fragments.
log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly.

The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

CONFIGURATION-EXTENDED-ACCESS-LIST

Command History

Version 9.4(0.0)	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platforms.
Version 9.3(0.0)	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.

Usage Information

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

Related Commands

ip access-list extended — creates an extended ACL.

permit tcp — assigns a permit filter for TCP packets.

permit udp — assigns a permit filter for UDP packets.

permit icmp

Configure a filter to allow all or specific ICMP messages.

Syntax

```
permit icmp {source mask | any | host ip-address} {destination
mask | any | host ip-address} [dscp] [message-type] [count
[byte]] [order] [fragments][log [interval minutes] [threshold-
in-msgs [count]] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq` *`sequence-number`* command if you know the filter’s sequence number.
- Use the `no permit icmp {`*`source mask`*` | any | host `*`ip-address`*`} {`*`destination mask`*` | any | host `*`ip-address`*`}` command.

Parameters

source	Enter the IP address of the network or host from which the packets were sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or noncontiguous.
any	Enter the keyword `any` to match and drop specific Ethernet traffic on the interface.
host *ip-address*	Enter the keyword `host` and then enter the IP address to specify a host IP address.
destination	Enter the IP address of the network or host to which the packets are sent.
dscp	Enter the keyword `dscp` to deny a packet based on the DSCP value. The range is 0 to 63.
message-type	(OPTIONAL) Enter an ICMP message type, either with the type (and code, if necessary) numbers or with the name of

	the message type. The range is 0 to 255 for ICMP type and 0 to 255 for ICMP code.
count	(OPTIONAL) Enter the keyword `count` to count packets the filter processes.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes the filter processes.
order	(OPTIONAL) Enter the keyword `order` to specify the QoS priority for the ACL entry. The range is 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). If you do not use the keyword `order`, the ACLs have the lowest order by default (**255**).
fragments	Enter the keyword `fragments` to use ACLs to control packet fragments.
log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

CONFIGURATION-IP ACCESS-LIST-STANDARD

Command History

Version 9.4(0.0)	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform.
Version 9.3(0.0)	Added the support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The `order` option is relevant in the context of the Policy QoS feature only. For more information, refer to the Quality of Service chapter of the *Dell Networking OS Configuration Guide*.

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

permit tcp

To pass TCP packets meeting the filter criteria, configure a filter.

Syntax

```
permit tcp {source mask | any | host ip-address} [bit]
[operator port [port]] {destination mask | any | host ip-
address} [bit] [dscp] [operator port [port]] [count [byte]]
[order] [fragments][log [interval minutes] [threshold-in-msgs
[count]] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq` *`sequence-number`* command if you know the filter's sequence number.
- Use the `no permit tcp {`*`source mask`*` | any | host `*`ip-address`*`} {`*`destination mask`*` | any | host `*`ip-address`*`}` command.

Parameters

source	Enter the IP address of the network or host from which the packets were sent.

mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword `host` then the IP address to specify a host IP address.
bit	Enter a flag or combination of bits: • `ack:` acknowledgement field • `fin:` finish (no more data from the user) • `psh:` push function • `rst:` reset the connection • `syn:` synchronize sequence numbers • `urg:` urgent field
dscp	Enter the keyword `dscp` to deny a packet based on the DSCP value. The range is from 0 to 63.
operator	(OPTIONAL) Enter one of the following logical operand: • `eq` = equal to • `neq` = not equal to • `gt` = greater than • `lt` = less than • `range` = inclusive range of ports (you must specify two ports for the port parameter)
port port	Enter the application layer port number. Enter two port numbers if you are using the range logical operand. The range is from 0 to 65535. The following list includes some common TCP port numbers: • 23 = Telnet • 20 and 21 = FTP • 25 = SMTP • 169 = SNMP
destination	Enter the IP address of the network or host to which the packets are sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
count	(OPTIONAL) Enter the keyword `count` to count packets the filter processes.

byte	(OPTIONAL) Enter the keyword `byte` to count bytes the filter processes.
order	(OPTIONAL) Enter the keyword `order` to specify the QoS priority for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). If you do not use the keyword `order`, the ACLs have the lowest order by default (**255**).
fragments	Enter the keyword `fragments` to use ACLs to control packet fragments.
log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or deny commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The threshold range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

CONFIGURATION-IP ACCESS-LIST-EXTENDED

Command History

Version 9.4(0.0)	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform.
Version 9.3(0.0)	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module platform.

Usage Information

The `order` option is relevant in the context of the Policy QoS feature only. For more information, refer to the “Quality of Service” chapter of the *Dell Networking OS Configuration Guide*.

The MXL 10/40GbE System IO Module cannot count both packets and bytes, so when you enter the count byte options, only bytes are incremented.

Most ACL rules require one entry in the CAM. However, rules with TCP and UDP port operators (for example, gt, lt, or range) may require more than one entry. The range of ports is configured in the CAM based on bit mask boundaries; the space required depends on exactly what ports are included in the range.

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

Example

An ACL rule with a TCP port range of 4000–8000 uses eight entries in the CAM.

```
Dell# Data             Mask         From To   #Covered

1 0000111110100000 1111111111100000 4000 4031 32
2 0000111111000000 1111111111000000 4032 4095 64
3 0001000000000000 1111100000000000 4096 6143 2048
4 0001100000000000 1111110000000000 6144 7167 1024
5 0001110000000000 1111111000000000 7168 7679 512
6 0001111000000000 1111111100000000 7680 7935 256
7 0001111100000000 1111111111000000 7936 7999 64
8 0001111101000000 1111111111111111 8000 8000 1

Total Ports: 4001
```

Example

An ACL rule with a TCP port lt 1023 uses only one entry in the CAM.

```
Dell# Data            Mask          From To   #Covered

1 0000000000000000 1111110000000000 0    1023 1024

Total Ports: 1024
```

Related Commands	[ip access-list extended]() — creates an extended ACL. [permit]() — assigns a permit filter for IP packets. [permit udp]() — assigns a permit filter for UDP packets.

permit udp

To pass UDP packets meeting the filter criteria, configure a filter.

Syntax

```
permit udp {source mask | any | host ip-address} [operator port
[port]] {destination mask | any | host ip-address} [dscp]
[operator port [port]] [count [byte]] [order] [fragments] [log
[interval minutes] [threshold-in-msgs [count]] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq` *`sequence-number`* command if you know the filter's sequence number.
- Use the `no permit udp {`*`source mask`*` | any | host `*`ip-address`*`} {`*`destination mask`*` | any | host `*`ip-address`* command.

Parameters

source	Enter the IP address of the network or host from which the packets were sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword `host` and then enter the IP address to specify a host IP address.
dscp	Enter the keyword `dscp` to deny a packet based on the DSCP value. The range is from 0 to 63.
operator	(OPTIONAL) Enter one of the following logical operand: • `eq` = equal to • `neq` = not equal to • `gt` = greater than • `lt` = less than • `range` = inclusive range of ports (you must specify two ports for the `port` parameter)
port port	Enter the application layer port number. Enter two port numbers if you are using the `range` logical operand. The range is 0 to 65535.

destination	Enter the IP address of the network or host to which the packets are sent.
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.
order	(OPTIONAL) Enter the keyword `order` to specify the QoS priority for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). If you do not use the keyword `order`, the ACLs have the lowest order by default (**255**).
fragments	Enter the keyword `fragments` to use ACLs to control packet fragments.
log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

CONFIGURATION-IP ACCESS-LIST-EXTENDED

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The `order` option is relevant in the context of the Policy QoS feature only. For more information, refer to the “Quality of Service” chapter of the *Dell Operating System Configuration Guide*.

In the MXL switch, you can configure either count (packets) or count (bytes). However, for an ACL with multiple rules, you can configure some ACLs with count (packets) and others as count (bytes) at any given time.

Most ACL rules require one entry in the CAM. However, rules with TCP and UDP port operators (for example, gt, lt, or range) may require more than one entry. The range of ports is configured in the CAM based on bit mask boundaries; the space required depends on exactly what ports are included in the range.

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

Example

An ACL rule with a TCP port range of 4000–8000 uses eight entries in the CAM.

```
Dell# Data             Mask         From To   #Covered

1 0000111110100000 1111111111100000 4000 4031 32
2 0000111111000000 1111111111000000 4032 4095 64
3 0001000000000000 1111100000000000 4096 6143 2048
4 0001100000000000 1111110000000000 6144 7167 1024
5 0001110000000000 1111111000000000 7168 7679 512
6 0001111000000000 1111111100000000 7680 7935 256
7 0001111100000000 1111111111000000 7936 7999 64
8 0001111101000000 1111111111111111 8000 8000 1

Total Ports: 4001
```

Example

An ACL rule with a TCP port lt 1023 uses only one entry in the CAM.

```
Dell# Data            Mask          From To   #Covered

1 0000000000000000 1111110000000000 0    1023 1024

Total Ports: 1024
```

Related Commands

ip access-list extended — creates an extended ACL.

permit — assigns a permit filter for IP packets.

permit tcp — assigns a permit filter for TCP packets.

seq

Assign a sequence number to a deny or permit filter in an extended IP access list while creating the filter.

Syntax

```
seq sequence-number {deny | permit} {ip-protocol-number | icmp
| ip | tcp | udp} {source mask | any | host ip-address}
{destination mask | any | host ip-address} [operator port
[port]] [count [byte]] [dscp value] [order] [fragments] [log
[interval minutes] [threshold-in-msgs [count]] [monitor]
```

Parameters

sequence-number	Enter a number from 0 to 4294967290. The range is from 1 to 65534.
deny	Enter the keyword `deny` to configure a filter to drop packets meeting this condition.
permit	Enter the keyword `permit` to configure a filter to forward packets meeting this criteria.
ip-protocol-number	Enter a number from 0 to 255 to filter based on the protocol identified in the IP protocol header.
icmp	Enter the keyword `icmp` to configure an ICMP access list filter.
ip	Enter the keyword `ip` to configure a generic IP access list. The keyword `ip` specifies that the access list permits all IP protocols.
tcp	Enter the keyword `tcp` to configure a TCP access list filter.
udp	Enter the keyword `udp` to configure a UDP access list filter.
source	Enter an IP address in dotted decimal format of the network from which the packet was received.
mask	(OPTIONAL) Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword `host` and then enter the IP address to specify a host IP address or hostname.

operator	(OPTIONAL) Enter one of the following logical operands: • `eq` = equal to • `neq` = not equal to • `gt` = greater than • `lt` = less than • `range` = inclusive range of ports (you must specify two ports for the `port` parameter.)
port port	(OPTIONAL) Enter the application layer port number. Enter two port numbers if you are using the range logical operand. The range is from 0 to 65535. The following list includes some common TCP port numbers: • 23 = Telnet • 20 and 21 = FTP • 25 = SMTP • 169 = SNMP
destination	Enter the IP address of the network or host to which the packets are sent.
count	(OPTIONAL) Enter the keyword `count` to count packets the filter processes.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes the filter processes.
dscp	(OPTIONAL) Enter the keyword `dcsp` to match to the IP DCSCP values.
order	(OPTIONAL) Enter the keyword `order` to specify the QoS order for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). If you do not use the keyword `order`, the ACLs have the lowest order by default (**255**).
fragments	Enter the keyword `fragments` to use ACLs to control packet fragments.
log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
threshold-in msgs count	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval minutes	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which the ACL logs must be generated. The interval range is from 1 to 10 minutes.

monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which the ACL logs are generated is five minutes. By default, the flow-based monitoring is not enabled.

Command Modes

CONFIGURATION-IP ACCESS-LIST-EXTENDED

Command History

Version 9.4(0.0)	Added support for the flow-based monitoring on the MXL 10/40GbE Switch IO Module.
Version 9.3(0.0)	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The `order` option is relevant in the context of the Policy QoS feature only. The following applies:

- The `seq` *`sequence-number`* command is applicable only in an ACL group.
- The `order` option works across ACL groups that have been applied on an interface via the QoS policy framework.
- The `order` option takes precedence over `seq` *`sequence-number`*.
- If *`sequence-number`* is not configured, the rules with the same order value are ordered according to their configuration order.
- If *`sequence-number`* is configured, the sequence-number is used as a tie breaker for rules with the same order.

If you configure the *`sequence-number`*, the *`sequence-number`* is used as a tie breaker for rules with the same order.

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

Related Commands

deny — Configures a filter to drop packets.

permit — Configures a filter to forward packets.

Common MAC Access List Commands

The following commands are available within both MAC ACL modes (Standard and Extended) and do not have mode-specific options. These commands allow you to clear, display, and assign MAC ACL configurations. The MAC ACL can be applied on Physical, Port-channel and VLAN interfaces. As per the stipulated rules in the ACL, the traffic on the Interface/VLAN members or Port-channel members will be permitted or denied.

The MXL 10/40GbE Switch IO Module platform supports both Ingress and Egress MAC ACLs.

clear counters mac access-group

Clear counters for all or a specific MAC ACL.

Syntax

```
clear counters mac access-group [mac-list-name]
```

Parameters

mac-list-name	(OPTIONAL) Enter the name of a configured MAC access list.

Command Modes

EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

mac access-group

Apply a MAC ACL to traffic entering or exiting an interface. Enter into the Interface mode and apply the MAC ACL in the following manner.

Syntax

```
mac access-group access-list-name {in [vlan vlan-range] | out}
```

To delete a MAC access-group, use the `no mac access-group mac-list-name` command.

Parameters

access-list-name	Enter the name of a configured MAC access list, up to 140 characters.
vlan *vlan-range*	(OPTIONAL) Enter the keyword `vlan` and then enter a range of VLANs. The range is from 1 to 4094 (you can use IDs 1 to 4094). NOTE: This option is available only with the keyword`in` option.
in	Enter the keyword `in` to configure the ACL to filter incoming traffic.
out	Enter the keyword `out` to configure the ACL to filter outgoing traffic.

Defaults

none

Command Modes

INTERFACE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

You can assign one ACL (standard or extended) to an interface.

In case of applying a MAC ACL to traffic entering or exiting a VLAN interface. Enter the VLAN interface mode and apply the mac acl in the following manner.

```
mac access-group access-list-name {in | out}
```

1. If the MAC ACL is applied on VLAN, none of the VLAN members should have an access list applied for that VLAN.
2. If the MAC ACL is applied on a Physical or Port Channel interface, the VLAN in which this port is associated should not have an access list applied.
3. If the MAC ACL is applied on a VLAN, then that VLAN should not belong to VLAN ACL group.
4. If the MAC ACL is applied on a VLAN ACL group, then none of the VLANs in that group should have an access list applied on it.

Related Commands

mac access-list standard — configures a standard MAC ACL.

mac access-list extended — configures an extended MAC ACL.

show mac access-lists

Display all of the Layer 2 ACLs configured in the system, whether or not they are applied to an interface, and the count of matches/mismatches against each ACL entry displayed.

Syntax

```
show mac access-lists [access-list-name] [interface interface]
[in | out]
```

Parameters

access-list-name	Enter the name of a configured MAC ACL, up to 140 characters.
interface *interface*	Enter the keyword `interface` then the one of the following keywords and slot/port or number information: • For a Port Channel interface, enter the keywords `port-channel` and then enter a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` and then enter the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` and then enter the slot/port information. • For a VLAN interface enter the keyword VLAN and then the *vlan id*.
in | out	Identify whether ACL is applied on ingress or egress side.

Command Modes

EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

show mac accounting access-list

Display MAC access list configurations and counters (if configured).

Syntax

```
show mac accounting access-list access-list-name interface
interface in | out
```

Parameters

access-list-name	Enter the name of a configured MAC ACL, up to 140 characters.
interface *interface*	Enter the keyword `interface` then the one of the following keywords and slot/port or number information: • For a Port Channel interface, enter the keywords `port-channel` and then enter a number. The range is from 1 to 128.

	- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` and then enter the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` and then enter the slot/port information. - For a VLAN interface enter the keyword VLAN and then the *vlan id*
in | out	Identify whether ACL is applied on ingress or egress side.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The ACL hit counters in this command increment the counters for each matching rule, not just the first matching rule.

Example

```
Dell#show mac accounting access-list TestMac interface
tengigabitethernet 0/89 in
Ingress Standard mac access-list TestMac on TenGigabitEthernet
0/89
Total cam count 2
seq 5 permit aa:aa:aa:aa:00:00 00:00:00:00:ff:ff count (0
packets)
seq 10 deny any count (20072594 packets)
Dell#
```

Standard MAC ACL Commands

When you create an access control list without any rule and then apply it to an interface, the ACL behavior reflects implicit permit. These commands configure standard MAC ACLs.

The MXL 10/40GbE Switch IO Module platform supports both Ingress and Egress MAC ACLs.

NOTE: For more information, also refer to the Commands Common to all ACL Types and Common MAC Access List Commands sections.

deny

To drop packets with a the MAC address specified, configure a filter.

Syntax

```
deny {any | mac-source-address [mac-source-address-mask]}
[count [byte]] [log [interval minutes] [threshold—in-msgs
[count]] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq` *`sequence-number`* command if you know the filter's sequence number.
- Use the `no deny {any |` *`mac-source-address mac-source-address-mask`*`}` command.

Parameters

any	Enter the keyword `any` to specify that all routes are subject to the filter.
mac-source-address	Enter a MAC address in nn:nn:nn:nn:nn:nn format.
mac-source-address-mask	(OPTIONAL) Specify which bits in the MAC address must match. If no mask is specified, a mask of 00:00:00:00:00:00 is applied (in other words, the filter allows only MAC addresses that match).
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword`log` to enable the triggering of ACL log messages.
threshold-in-msgs *count*	(OPTIONAL) Enter the`threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated. with the seq, permit, or deny commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The threshold range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

CONFIGURATION-MAC ACCESS LIST-STANDARD

Command History

Version 9.4(0.0)	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform.
Version 9.3(0.0)	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module platform.

Usage Information

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

Related Commands

permit — configures a MAC address filter to pass packets.

seq — configures a MAC address filter with a specified sequence number.

mac access-list standard

To configure a standard MAC ACL, name a new or existing MAC access control list (MAC ACL) and enter MAC ACCESS LIST mode.

Syntax

```
mac access-list standard mac-list-name
```

Parameters

mac-list-name	Enter a text string as the name of the standard MAC access list (140 character maximum).

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History	**Version 8.3.16.1**	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The Dell operating system supports one ingress and one egress MAC ACL per interface.

The number of entries allowed per ACL is hardware-dependent. For detailed specification about entries allowed per ACL, refer to your switch documentation.

The MXL Switch supports both ingress and egress ACLs.

Example

```
Dell(conf)#mac-access-list access-list standard TestMAC
Dell(config-std-macl)#permit 00:00:00:00:00:00
00:00:00:00:ff:ff count
Dell(config-std-macl)#deny  any count
```

permit

To forward packets from a specific source MAC address, configure a filter.

Syntax

```
permit {any | mac-source-address [mac-source-address-mask]}
[count [byte]] | log [interval minutes] [threshold-in-
msgs[count] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq` *`sequence-number`* command if you know the filter's sequence number.
- Use the `no permit {any |` *`mac-source-address mac-source-address-mask`*`}` command.

Parameters

any	Enter the keyword `any` to forward all packets received with a MAC address.
mac-source-address	Enter a MAC address in nn:nn:nn:nn:nn:nn format.
mac-source-address-mask	(OPTIONAL) Specify which bits in the MAC address must match. If no mask is specified, a mask of 00:00:00:00:00:00 is applied (in other words, the filter allows only MAC addresses that match).
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.

threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-`*`msgs`* keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface

Defaults Not configured.

Command Modes CONFIGURATION-MAC ACCESS LIST-STANDARD

Command History

Version 9.4(0.0)	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform.
Version 9.3(0.0)	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

When the configured maximum threshold is exceeded, generation of logs are stopped.

When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, Pv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

Related Commands

deny — configures a MAC ACL filter to drop packets.

seq —configure a MAC ACL filter with a specified sequence number.

seq

To a deny or permit filter in a MAC access list while creating the filter, assign a sequence number.

Syntax

```
seq sequence-number {deny | permit} {any | mac-source-address
[mac-source-address-mask]} [count [byte]] [log [interval
minutes] [threshold-in-msgs [count]] [monitor]
```

To remove this filter, use the `no seq sequence-number` command.

Parameters

sequence-number	Enter a number from 0 to 65535.
deny	Enter the keyword `deny` to configure a filter to drop packets meeting this condition.
permit	Enter the keyword `permit` to configure a filter to forward packets meeting this criteria.
any	Enter the keyword `any` to filter all packets.
mac-source-address	Enter a MAC address in nn:nn:nn:nn:nn:nn format.
mac-source-address-mask	(OPTIONAL) Specify which bits in the MAC address must match. If no mask is specified, a mask of 00:00:00:00:00:00 is applied (in other words, the filter allows only MAC addresses that match).
count	(OPTIONAL) Enter the keyword `count` to count packets the filter processes.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes the filter processes.
log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.

interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes..
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

CONFIGURATION-MAC ACCESS LIST-STANDARD

Command History

Version 9.4(0.0)	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform.
Version 9.3(0.0)	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

Related Commands

deny — configures a filter to drop packets.

permit — configures a filter to forward packets.

Extended MAC ACL Commands

When an access-list is created without any rule and then applied to an interface, ACL behavior reflects implicit permit. The following commands configure Extended MAC ACLs.

The MXL 10/40GbE Switch IO Module platform supports both Ingress and Egress MAC ACLs.

deny

To drop packets that match the filter criteria, configure a filter.

Syntax

`deny {any | host mac-address | mac-source-address mac-source-address-mask} {any | host mac-address | mac-destination-address mac-destination-address-mask} [ethertype-operator] [count [byte]]`

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no deny {any | host mac-address | mac-source-address mac-source-address-mask} {any | host mac-address | mac-destination-address mac-destination-address-mask}` command.

Parameters

any	Enter the keyword `any` to drop all packets.
host *mac-address*	Enter the keyword `host` and then enter a MAC address to drop packets with that host address.
mac-source-address	Enter a MAC address in nn:nn:nn:nn:nn:nn format.
mac-source-address-mask	Specify which bits in the MAC address must match. The MAC ACL supports an inverse mask; therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
mac-destination-address	Enter the destination MAC address and mask in nn:nn:nn:nn:nn:nn format.

mac-destination-address-mask	Specify which bits in the MAC address must match. The MAC ACL supports an inverse mask; therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
ethertype operator	(OPTIONAL) To filter based on protocol type, enter one of the following Ethertypes: • `ev2` - is the Ethernet II frame format • `llc` - is the IEEE 802.3 frame format • `snap` - is the IEEE 802.3 SNAP frame format
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.

Defaults Not configured.

Command Modes CONFIGURATION-MAC ACCESS LIST-EXTENDED

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

permit — configures a MAC address filter to pass packets.

seq — configures a MAC address filter with a specified sequence number.

mac access-list extended

Name a new or existing extended MAC access control list (extended MAC ACL).

Syntax `mac access-list extended access-list-name [cpu-qos]`

Parameters

access-list-name	Enter a text string as the MAC access list name, up to 140 characters.
cpu-qos	Enter the keyword `cpu-qos` to assign this ACL to control plane traffic only (CoPP).

Defaults None

Command Modes CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The number of entries allowed per ACL is hardware-dependent. For detailed specifications on entries allowed per ACL, refer to your line card documentation.

Example

```
Dell(conf)#mac-access-list access-list extended TestMATExt
Dell(config-ext-macl)#remark 5 IPv4
Dell(config-ext-macl)#seq 10 permit any any ev2 eq 800 count
bytes
Dell(config-ext-macl)#remark 15 ARP
Dell(config-ext-macl)#seq 20 permit any any ev2 eq 806 count
bytes
Dell(config-ext-macl)#remark 25 IPv6
Dell(config-ext-macl)#seq 30 permit any any ev2 eq 86dd count
bytes
Dell(config-ext-macl)#seq 40 permit any any count bytes
Dell(config-ext-macl)#exit
Dell(conf)#do show mac accounting access-list snickers
interface g0/47 in
Extended mac access-list snickers on GigabitEthernet 0/47
seq 10 permit any any ev2 eq 800 count bytes (559851886
packets 191402152148bytes)seq 20 permit any any ev2 eq 806
count bytes
(74481486 packets 5031686754bytes)seq 30 permit any any ev2 eq
86dd count bytes (7751519 packets 797843521 bytes)
```

Related Commands

mac access-list standard — configures a standard MAC access list.

show mac accounting access-list — displays MAC access list configurations and counters (if configured).

permit

To pass packets matching the criteria specified, configure a filter.

Syntax

`permit {any | host` *`mac-address`* `|` *`mac-source-address mac-source-address-mask`*`} {any | host` *`mac-address`* `|` *`mac-destination-address mac-destination-address-mask`*`} [`*`ethertype operator`*`] [count [byte]]`

To remove this filter, you have two choices:

- Use the `no seq` *`sequence-number`* command if you know the filter's sequence number.
- Use the `no permit {any | host` *`mac-address`* `|` *`mac-source-address mac-source-address-mask`*`} {any |` *`mac-destination-address mac-destination-address-mask`*`}` command.

Parameters

any	Enter the keyword `any` to forward all packets.
host	Enter the keyword `host` then a MAC address to forward packets with that host address.
mac-source-address	Enter a MAC address in nn:nn:nn:nn:nn:nn format.
mac-source-address-mask	(OPTIONAL) Specify which bits in the MAC address must match. The MAC ACL supports an inverse mask; therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
mac-destination-address	Enter the destination MAC address and mask in nn:nn:nn:nn:nn:nn format.
mac-destination-address-mask	Specify which bits in the MAC address must be matched. The MAC ACL supports an inverse mask; therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
ethertype operator	(OPTIONAL) To filter based on protocol type, enter one of the following Ethertypes: • `ev2` - is the Ethernet II frame format • `llc` - is the IEEE 802.3 frame format • `snap` - is the IEEE 802.3 SNAP frame format
count	(OPTIONAL) Enter the keyword `count` to count packets the filter processes.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes the filter processes.

Defaults

Not configured.

Command Modes

CONFIGURATION-MAC ACCESS LIST-EXTENDED

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

deny — configures a MAC ACL filter to drop packets.

seq — configure a MAC ACL filter with a specified sequence number.

seq

Configure a filter with a specific sequence number.

Syntax

```
seq sequence-number {deny | permit} {any | host mac-address |
mac-source-address mac-source-address-mask} {any | host mac-
address | mac-destination-address mac-destination-address-mask}
[ethertype operator] [count [byte]]
```

Parameters

sequence-number	Enter a number as the filter sequence number. The range is from zero (0) to 65535.
deny	Enter the keyword `deny` to drop any traffic matching this filter.
permit	Enter the keyword `permit` to forward any traffic matching this filter.
any	Enter the keyword `any` to filter all packets.
host *mac-address*	Enter the keyword `host` and then enter a MAC address to filter packets with that host address.
mac-source-address	Enter a MAC address in nn:nn:nn:nn:nn:nn format. The MAC ACL supports an inverse mask; therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
mac-source-address-mask	Specify which bits in the MAC address must be matched.
mac-destination-address	Enter the destination MAC address and mask in nn:nn:nn:nn:nn:nn format.
mac-destination-address-mask	Specify which bits in the MAC address must be matched. The MAC ACL supports an inverse mask; therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
ethertype operator	(OPTIONAL) To filter based on protocol type, enter one of the following Ethertypes: • `ev2` - is the Ethernet II frame format. • `llc` - is the IEEE 802.3 frame format. • `snap` - is the IEEE 802.3 SNAP frame format.
count	(OPTIONAL) Enter the keyword `count` to count packets the filter processes.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes the filter processes.

Defaults	Not configured.
Command Modes	CONFIGURATION-MAC ACCESS LIST-STANDARD
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	deny — configures a filter to drop packets. permit — configures a filter to forward packets.

IP Prefix List Commands

When you create an access-list without any rule and then apply it to an interface, the ACL behavior reflects implicit permit.

To configure or enable IP prefix lists, use these commands.

clear ip prefix-list

Reset the number of times traffic mets the conditions ("hit" counters) of the configured prefix lists.

Syntax	`clear ip prefix-list [prefix-name]`
Parameters	***prefix-name*** (OPTIONAL) Enter the name of the configured prefix list to clear only counters for that prefix list, up to 140 characters long.
Defaults	Clears "hit" counters for all prefix lists unless a prefix list is specified.
Command Modes	EXEC Privilege
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	ip prefix-list — configures a prefix list.

deny

To drop packets meeting the criteria specified, configure a filter.

Syntax	`deny ip-prefix [ge min-prefix-length] [le max-prefix-length]`

Parameters

ip-prefix	Specify an IP prefix in the network/length format. For example, 35.0.0.0/ 8 means match the first 8 bits of address 35.0.0.0.
ge *min-prefix-length*	(OPTIONAL) Enter the keyword `ge` and then enter the minimum prefix length, which is a number from zero (0) to 32.
le *max-prefix-length*	(OPTIONAL) Enter the keyword `le` and then enter the maximum prefix length, which is a number from zero (0) to 32.

Defaults

Not configured.

Command Modes

PREFIX-LIST

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Sequence numbers for this filter are automatically assigned starting at sequence number 5.

If you do not use the `ge` or `le` options, only packets with an exact match to the prefix are filtered.

Related Commands

permit — configures a filter to pass packets.

seq — configures a drop or permit filter with a specified sequence number.

ip prefix-list

Enter the PREFIX-LIST mode and configure a prefix list.

Syntax

`ip prefix-list prefix-name`

Parameters

prefix-name	Enter a string up to 16 characters long as the name of the prefix list, up to 140 characters long.

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Prefix lists redistribute OSPF and RIP routes meeting specific criteria.

Related Commands	show ip route list — displays IP routes in an IP prefix list. show ip prefix-list summary — displays a summary of the configured prefix lists.

permit

Configure a filter that passes packets meeting the criteria specified.

Syntax

```
permit ip-prefix [ge min-prefix-length] [le max-prefix-length]
```

Parameters

ip-prefix	Specify an IP prefix in the network/length format. For example, 35.0.0.0/8 means match the first 8 bits of address 35.0.0.0.
ge *min-prefix-length*	(OPTIONAL) Enter the keyword `ge` and then enter the minimum prefix length, which is a number from zero (0) to 32.
le *max-prefix-length*	(OPTIONAL) Enter the keyword `le` and then enter the maximum prefix length, which is a number from zero (0) to 32.

Command Modes: PREFIX-LIST

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Sequence numbers for this filter are automatically assigned starting at sequence number 5.

If you do not use the `ge` or `le` options, only packets with an exact match to the prefix are filtered.

Related Commands

deny — configures a filter to drop packets.

seq — configures a drop or permit filter with a specified sequence number.

seq

To a deny or permit filter in a prefix list while configuring the filter, assign a sequence number.

Syntax

```
seq sequence-number {deny | permit} {any} | [ip-prefix /nn {ge
min-prefix-length} {le max-prefix-length}] | [bitmask number]
```

Parameters	*sequence-number*	Enter a number. The range is from 1 to 4294967294.
	deny	Enter the keyword `deny` to configure a filter to drop packets meeting this condition..
	permit	Enter the keyword `permit` to configure a filter to forward packets meeting this condition.
	any	(OPTIONAL) Enter the keyword `any` to match any packets.
	ip-prefix /nn	(OPTIONAL) Specify an IP prefix in the network/length format. For example, 35.0.0.0/8 means match the first 8 bits of address 35.0.0.0.
	ge *min-prefix-length*	(OPTIONAL) Enter the keyword `ge` and then enter the minimum prefix length, which is a number from zero (0) to 32.
	le *max-prefix-length*	(OPTIONAL) Enter the keyword `le` and then enter the maximum prefix length, which is a number from zero (0) to 32.
	bitmask *number*	Enter the keyword `bitmask` then enter a bit mask number in dotted decimal format.

Defaults	Not configured.
Command Modes	PREFIX-LIST

Command History	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information	If you do not use the `ge` or `le` options, only packets with an exact match to the prefix are filtered.
Related Commands	deny — configures a filter to drop packets. permit — configures a filter to pass packets.

show config

Display the current PREFIX-LIST configurations.

Syntax	`show config`
Command Modes	PREFIX-LIST

Command History	**Version 8.3.16.1**	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell(conf-nprefixl)#show config
!
ip prefix-list snickers
Dell(conf-nprefixl)#
```

show ip prefix-list detail

Display details of the configured prefix lists.

Syntax `show ip prefix-list detail [`*`prefix-name`*`]`

Parameters

prefix-name	(OPTIONAL) Enter a text string as the name of the prefix list, up to 140 characters.

Command Modes

- EXEC
- EXEC Privilege

Command History	**Version 8.3.16.1**	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show ip prefix-list detail
Ip Prefix-list with the last deletion/insertion: PL_OSPF_to_RIP
ip prefix-list PL_OSPF_to_RIP:
count: 3, range entries: 1, sequences: 5 - 25
   seq 5 permit 1.1.1.0/24 (hit count: 0)
   seq 10 deny 2.1.0.0/16 ge 23 (hit count: 0)
   seq 25 permit 192.0.0.0 bitmask 192.0.0.0 (hit count: 800)
```

show ip prefix-list summary

Display a summary of the configured prefix lists.

Syntax `show ip prefix-list summary [`*`prefix-name`*`]`

Parameters

prefix-name	(OPTIONAL) Enter a text string as the name of the prefix list, up to 140 characters.

Command Modes

- EXEC
- EXEC Privilege

Command History	**Version 8.3.16.1**	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show ip prefix-list summary
Ip Prefix-list with the last deletion/insertion: PL_OSPF_to_RIP
ip prefix-list PL_OSPF_to_RIP:
count: 3, range entries: 1, sequences: 5 - 25
```

Route Map Commands

When you create an access-list without any rule and then applied to an interface, the ACL behavior reflects implicit permit.

To configure route maps and their redistribution criteria, use the following commands.

continue

To a route-map entry with a higher sequence number, configure a route-map.

Syntax `continue [sequence-number]`

Parameters

sequence-number	(OPTIONAL) Enter the route map sequence number. The range is from 1 to 65535. The default is: no sequence number

Defaults Not configured

Command Modes ROUTE-MAP

Command History	**Version 8.3.16.1**	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The `continue` feature allows movement from one route-map entry to a specific route-map entry (the sequence number). If you do not specify the sequence number, the `continue` feature simply moves to the next sequence number (also known as an implied continue). If a match clause exists, the `continue` feature executes only after a successful match occurs. If there are no successful matches, the `continue` feature is ignored.

Match clause with Continue clause

The `continue` feature can exist without a match clause. A continue clause without a match clause executes and jumps to the specified route-map entry.

With a match clause and a continue clause, the match clause executes first and the continue clause next in a specified route map entry. The continue clause launches only after a successful match. The behavior is:

- A successful match with a continue clause, the route map executes the set clauses and then goes to the specified route map entry upon execution of the continue clause.
- If the next route map entry contains a continue clause, the route map executes the continue clause if a successful match occurs.
- If the next route map entry does not contain a continue clause, the route map evaluates normally. If a match does not occur, the route map does not continue and falls through to the next sequence number, if one exists.

Set Clause with Continue Clause

If the route-map entry contains sets with the continue clause, set actions are performed first then the continue clause jumps to the specified route map entry.

- If a set action occurs in the first route map entry and then the same set action occurs with a different value in a subsequent route map entry, the last set of actions overrides the previous set of actions with the same `set` command.
- If `set community additive` and `set as-path prepend` are configure, the communities and AS numbers are prepended.

Related Commands	set metric — Specifies a COMMUNITY attribute set automatic-tag — Configures a filter to modify the AS path

description

Add a description to this route map.

Syntax	`description description`
Parameters	*description* Enter a description to identify the route map (80 characters maximum).
Defaults	none
Command Modes	ROUTE-MAP
Command History	Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	route-map — Enables a route map.

match interface

To match routes whose next hop is on the interface specified, configure a filter.

Syntax	`match interface interface` To remove a match, use the `no match interface interface` command.

Parameters

interface	Enter the following keywords and slot/port or number information: • For the Loopback interface, enter the keyword `loopback` then a number from zero (0) to 16383. • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a Ten Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

Defaults	Not configured.
Command Modes	ROUTE-MAP

Command History

Version 8.3.16.0	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

match ip address — redistributes routes that match an IP address.

match ip next-hop — redistributes routes that match the next-hop IP address.

match ip route-source — redistributes routes that match routes advertised by other routers.

match metric — redistributes routes that match a specific metric.

match route-type — redistributes routes that match a route type.

match tag — redistributes routes that match a specific tag.

match ip address

To match routes based on IP addresses specified in an access list, configure a filter.

Syntax	`match ip address prefix-list-name`

Parameters

prefix-list-name	Enter the name of configured prefix list, up to 140 characters.

Defaults Not configured.

Command Modes ROUTE-MAP

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

match interface — redistributes routes that match the next-hop interface.

match ip next-hop — redistributes routes that match the next-hop IP address.

match ip route-source — redistributes routes that match routes advertised by other routers.

match metric — redistributes routes that match a specific metric.

match route-type — redistributes routes that match a route type.

match tag — redistributes routes that match a specific tag.

match ip next-hop

To match based on the next-hop IP addresses specified in an IP access list or IP prefix list, configure a filter.

Syntax `match ip next-hop {access-list | prefix-list prefix-list-name}`

Parameters

access-list-name	Enter the name of a configured IP access list, up to 140 characters.
prefix-list *prefix-list-name*	Enter the keywords `prefix-list` and then enter the name of configured prefix list, up 10 140 characters.

Defaults Not configured.

Command Modes ROUTE-MAP

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

match interface — redistributes routes that match the next-hop interface.

match ip address — redistributes routes that match an IP address.

match ip route-source — redistributes routes that match routes advertised by other routers.

match metric — redistributes routes that match a specific metric.

match route-type — redistributes routes that match a route type.

match tag — redistributes routes that match a specific tag.

match ip route-source

To match based on the routes advertised by routes specified in IP access lists or IP prefix lists, configure a filter.

Syntax

`match ip route-source {access-list | prefix-list prefix-list-name}`

Parameters

access-list-name	Enter the name of a configured IP access list, up to 140 characters.
prefix-list *prefix-list-name*	Enter the keywords `prefix-list` and then enter the name of configured prefix list, up to 140 characters.

Defaults

Not configured.

Command Modes

ROUTE-MAP

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

match interface — redistributes routes that match the next-hop interface.

match ip address — redistributes routes that match an IP address.

match ip next-hop — redistributes routes that match the next-hop IP address.

match metric — redistributes routes that match a specific metric.

match route-type — redistributes routes that match a route type.

match tag — redistributes routes that match a specific tag.

match metric

To match on a specified value, configure a filter.

Syntax	`match metric metric-value`
Parameters	*metric-value*: Enter a value to match. The range is from zero (0) to 4294967295.
Defaults	Not configured.
Command Modes	ROUTE-MAP
Command History	Version 8.3.16.1: Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

match interface — redistributes routes that match the next-hop interface.

match ip address — redistributes routes that match an IP address.

match ip next-hop — redistributes routes that match the next-hop IP address.

match ip route-source — redistributes routes that match routes advertised by other routers.

match route-type — redistributes routes that match a route type.

match tag — redistributes routes that match a specific tag.

match route-type

To match routes based on the how the route is defined, configure a filter.

Syntax

```
match route-type {external [type-1 | type-2] | internal |
local}
```

Parameters

external [type-1| type-2]	Enter the keyword `external` then either type-1 or type-2 to match only on OSPF Type 1 routes or OSPF Type 2 routes.
internal	Enter the keyword `internal` to match only on routes generated within OSPF areas.
local	Enter the keyword `local` to match only on routes generated within the switch.

Defaults	Not configured.
Command Modes	ROUTE-MAP

Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	match interface — redistributes routes that match the next-hop interface. match ip address — redistributes routes that match an IP address. match ip next-hop — redistributes routes that match the next-hop IP address. match ip route-source — redistributes routes that match routes advertised by other routers. match metric — redistributes routes that match a specific metric. match tag — redistributes routes that match a specific tag.

match tag

To redistribute only routes that match a specified tag value, configure a filter.

Syntax	`match tag tag-value`
Parameters	***tag-value*** Enter a value as the tag on which to match. The range is from zero (0) to 4294967295.
Defaults	Not configured.
Command Modes	ROUTE-MAP
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	match interface — redistributes routes that match the next-hop interface. match ip address — redistributes routes that match an IP address. match ip next-hop — redistributes routes that match the next-hop IP address. match ip route-source — redistributes routes that match routes advertised by other routers. match metric — redistributes routes that match a specific metric. match route-type — redistributes routes that match a route type.

route-map

Enable a route map statement and configure its action and sequence number. This command also places you in ROUTE-MAP mode.

Syntax

`route-map map-name [permit | deny] [sequence-number]`

Parameters

map-name	Enter a text string of up to 140 characters to name the route map for easy identification.
permit	(OPTIONAL) Enter the keyword `permit` to set the route map default as permit. If you do not specify a keyword, the default is `permit`.
deny	(OPTIONAL) Enter the keyword `deny` to set the route map default as deny.
sequence-number	(OPTIONAL) Enter a number to identify the route map for editing and sequencing with other route maps. You are prompted for a sequence number if there are multiple instances of the route map. The range is from 1 to 65535.

Defaults

Not configured.

If you do not define a keyword (`permit` or `deny`) for the route map, the `permit` action is the default.

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module

Usage Information

Use caution when you delete route maps because if you do not specify a sequence number, all route maps with the same *map-name* are deleted when you use the `no route-map map-name` command.

Example

```
Dell(conf)#route-map dempsey
Dell(config-route-map)#
```

Related Commands

show config2 — displays the current configuration.

set automatic-tag

To automatically compute the tag value of the route, configure a filter.

Syntax

`set automatic-tag`

To return to the default, use the `no set automatic-tag` command.

Defaults	Not configured.
Command Modes	ROUTE-MAP
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	set metric — specify the metric value assigned to redistributed routes. set metric-type — specify the metric type assigned to redistributed routes. set tag — specify the tag assigned to redistributed routes.

set metric

To assign a new metric to redistributed routes, configure a filter.

Syntax

`set metric [+ | -] metric-value`

To delete a setting, use the `no set metric` command.

Parameters

+	(OPTIONAL) Enter + to add a metric-value to the redistributed routes.
-	(OPTIONAL) Enter – to subtract a metric-value from the redistributed routes.
metric-value	Enter a number as the new metric value. The range is from zero (0) to 4294967295.

Defaults	Not configured.
Command Modes	ROUTE-MAP
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	set automatic-tag — computes the tag value of the route. set metric-type — specifies the route type assigned to redistributed routes. set tag — specifies the tag assigned to redistributed routes.

set metric-type

To assign a new route type for routes redistributed to OSPF, configure a filter.

Syntax `set metric-type {internal | external | type-1 | type-2}`

Parameters

internal	Enter the keyword `internal` to assign the Interior Gateway Protocol metric of the next hop as the route's BGP MULTI_EXIT_DES (MED) value.
external	Enter the keyword `external` to assign the IS-IS external metric.
type-1	Enter the keyword `type-1` to assign the OSPF Type 1 metric.
type-2	Enter the keyword `type-2` to assign the OSPF Type 2 metric.

Defaults Not configured.

Command Modes ROUTE-MAP

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

set automatic-tag — computes the tag value of the route.

set metric — specifies the metric value assigned to redistributed routes.

set tag — specifies the tag assigned to redistributed routes.

set tag

To specify a tag for redistributed routes, configure a filter.

Syntax `set tag tag-value`

Parameters

tag-value	Enter a number as the tag. The range is from zero (0) to 4294967295.

Defaults Not configured.

Command Modes ROUTE-MAP

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

set automatic-tag — computes the tag value of the route.

set metric — specifies the metric value assigned to redistributed routes.

set metric-type — specifies the route type assigned to redistributed routes.

show config

Display the current route map configuration.

Syntax	`show config`
Command Modes	ROUTE-MAP
Command History	**Version 8.3.16.1** Introduced on MXL 10/40GbE Switch IO Module

Example

```
Dell(config-route-map)#show config
!
route-map hopper permit 10
Dell(config-route-map)#
```

show route-map

Display the current route map configurations.

Syntax `show route-map [map-name]`

Parameters

map-name	(OPTIONAL) Enter the name of a configured route map, up to 140 characters.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show route-map
route-map firpo, permit, sequence 10
 Match clauses:
 Set clauses:
  tag 34
Dell#
```

Related Commands route-map — configures a route map.

deny (for Standard IP ACLs)

To drop packets with a certain IP address, configure a filter.

Syntax

`deny {source | any | host {ip-address}}[count [byte]] [dscp value] [order] [fragments] [log [interval minutes] [threshold-in-msgs [count]] [monitor]`

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no deny {source [mask] | any | host ip-address}` command.

Parameters

source	Enter the IP address of the network or host from which the packets were sent.
any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword `host` then the IP address to specify a host IP address.
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.
dscp	Enter this keyword `dscp` to deny a packet based on the DSCP value. The range is from 0 to 63.
log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
order	(OPTIONAL) Enter the keyword `order` to specify the QoS priority for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority) If you did not use the keyword order, the ACLs have the lowest order by default (255).
fragments	Enter the keyword `fragments` to use ACLs to control packet fragments.
threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.

monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly.

The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

CONFIGURATION-STANDARD-ACCESS-LIST

Command History

Version 9.4(0.0)	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platforms.
Version 9.3(0.0)	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module platforms.

Usage Information

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

Related Commands

ip access-list standard — configures a standard ACL.

permit — configures a permit filter.

deny (for Extended IP ACLs)

Configure a filter that drops IP packets meeting the filter criteria.

Syntax

```
deny {ip | ip-protocol-number} {source mask | any | host ip-
address} {destination mask | any | host ip-address} [count
[byte]] [dscp value] [order] [monitor] [fragments] [log
[interval minutes] [threshold-in-msgs [count]] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no deny {ip | ip-protocol-number} {source mask | any | host ip-address} {destination mask | any | host ip-address}` command.

Parameters

source	Enter the IP address of the network or host from which the packets were sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword `host` then the IP address to specify a host IP address.
destination	Enter the IP address of the network or host to which the packets are sent.
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.
order	(OPTIONAL) Enter the keyword `order` to specify the QoS priority for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority) If you did not use the keyword `order`, the ACLs have the lowest order by default (255).
monitor	OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.
fragments	Enter the keyword `fragments` to use ACLs to control packet fragments.
log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.

threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The time interval range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly.

The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

CONFIGURATION-EXTENDED-ACCESS-LIST

Command History

Version 9.4(0.0)	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform.
Version 9.3(0.0)	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.

Usage Information

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

Related Commands	
	deny tcp — assigns a filter to deny TCP packets. deny udp — assigns a filter to deny UDP packets. ip access-list extended — creates an extended ACL.

seq

Assign a sequence number to a deny or permit filter in an extended IP access list while creating the filter.

Syntax

```
seq sequence-number {deny | permit} {source [mask] | any | host
ip-address}} [count [byte] [dscp value] [order] [fragments]
[log [interval minutes] [threshold-in-msgs [count] [monitor]
```

Parameters

sequence-number	Enter a number from 0 to 4294967290. The range is from 0 to 65534.
deny	Enter the keyword `deny` to configure a filter to drop packets meeting this condition.
permit	Enter the keyword `permit` to configure a filter to forward packets meeting this criteria.
source	Enter an IP address in dotted decimal format of the network from which the packet was received.
mask	(OPTIONAL) Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword `any` to specify that all routes are subject to the filter.
count	(OPTIONAL) Enter the keyword `count` to count packets the filter processes.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes the filter processes.
dscp	(OPTIONAL) Enter the keyword `dcsp` to match to the IP DCSCP values.
order	(OPTIONAL) Enter the keyword `order` to specify the QoS order for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). If you do not use the keyword `order`, the ACLs have the lowest order by default (**255**).
fragments	Enter the keyword `fragments` to use ACLs to control packet fragments.

log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
threshold-in *msgs* count	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` then by the time period in minutes at which the ACL logs must be generated. The interval range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

CONFIGURATION-IP ACCESS-LIST-STANDARD

Command History

Version 9.4(0.0)	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform.
Version 9.3(0.0)	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The `order` option is relevant in the context of the Policy QoS feature only. The following applies:

- The `seq` *`sequence-number`* command is applicable only in an ACL group.
- The `order` option works across ACL groups that have been applied on an interface via the QoS policy framework.
- The `order` option takes precedence over `seq` *`sequence-number`*.
- If *`sequence-number`* is not configured, the rules with the same order value are ordered according to their configuration order.
- If *`sequence-number`* is configured, the sequence-number is used as a tie breaker for rules with the same order.

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

Related Commands

deny — configures a filter to drop packets.

permit — configures a filter to forward packets.

seq — assigns a sequence number to a deny or permit filter in an IP access list while creating the filter.

deny tcp

Configure a filter that drops transmission control protocol (TCP) packets meeting the filter criteria.

Syntax

```
deny tcp {source mask | any | host ip-address} [bit] [operator
port [port]] {destination mask | any | host ip-address} [dscp]
[bit] [operator port [port]] [count [byte] [order] [fragments]
[log [interval minutes] [threshold-in-msgs [count]] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq` *`sequence-number`* command if you know the filter's sequence number.
- Use the `no deny tcp {`*`source mask`*` | any | host `*`ip-address`*`} {`*`destination mask`*` | any | host `*`ip-address`*`}` command.

Parameters

source	Enter the IP address of the network or host from which the packets are sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword `any` to specify that all routes are subject to the filter.

host *ip-address*	Enter the keyword `host` then the IP address to specify a host IP address.
dscp	Enter this keyword `dscp` to deny a packet based on the DSCP value. The range is from 0 to 63.
bit	Enter a flag or combination of bits: • `ack:` acknowledgement field • `fin:` finish (no more data from the user) • `psh:` push function • `rst:` reset the connection • `syn:` synchronize sequence numbers • `urg:` urgent field
operator	(OPTIONAL) Enter one of the following logical operand: • `eq` = equal to • `neq` = not equal to • `gt` = greater than • `lt` = less than • `range` = inclusive range of ports (you must specify two ports for the `port` command)
port port	Enter the application layer port number. Enter two port numbers if using the range logical operand. The range is from 0 to 65535. The following list includes some common TCP port numbers: • 23 = Telnet • 20 and 21 = FTP • 25 = SMTP • 169 = SNMP
destination	Enter the IP address of the network or host to which the packets are sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
count	(OPTIONAL) Enter the keyword `count` to count packets the filter processes.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes the filter processes.
order	(OPTIONAL) Enter the keyword `order` to specify the QoS priority for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order

	numbers have a higher priority) If you did not use the keyword `order`, the ACLs have the lowest order by default (**255**).
fragments	Enter the keyword `fragments` to use ACLs to control packet fragments.
log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
threshold-in-msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly.

The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

CONFIGURATION-IP ACCESS-LIST-EXTENDED

Command History

9.4(0.0)	Added the support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platforms.
9.3(0.0)	Added the support for logging of ACLs on the MXL 10/40GbE Switch IO Module platforms.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The `order` option is relevant in the context of the Policy QoS feature only. For more information, refer to the Quality of Service chapter of the *Dell Networking OS Configuration Guide*.

In the MXL switch, you can configure either count (packets) or count (bytes). However, for an ACL with multiple rules, you can configure some ACLs with count (packets) and others as count (bytes) at any given time.

Most ACL rules require one entry in the CAM. However, rules with TCP and UDP port operators (for example, gt, lt, or range) may require more than one entry. The range of ports is configured in the CAM based on bit mask boundaries; the space required depends on exactly what ports are included in the range.

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

Example

An ACL rule with a TCP port range of 4000–8000 uses eight entries in the CAM.

```
Dell#  Data             Mask        From To #Covered

1 0000111110100000 1111111111100000 4000 4031 32
2 0000111111000000 1111111111000000 4032 4095 64
3 0001000000000000 1111100000000000 4096 6143 2048
4 0001100000000000 1111110000000000 6144 7167 1024
5 0001110000000000 1111111000000000 7168 7679 512
6 0001111000000000 1111111100000000 7680 7935 256
7 0001111100000000 1111111111000000 7936 7999 64
8 0001111101000000 1111111111111111 8000 8000 1

Total  Ports: 4001
```

Example

An ACL rule with a TCP port lt 1023 uses only one entry in the CAM.

```
Dell# Data              Mask        From To   #Covered

1 0000000000000000 1111110000000000 0    1023 1024

Total  Ports: 1024
```

Related Commands

deny — assigns a filter to deny IP traffic.

deny udp — assigns a filter to deny UDP traffic.

deny udp

To drop user datagram protocol (UDP) packets meeting the filter criteria, configure a filter.

Syntax

```
deny udp {source mask | any | host ip-address} [operator port
[port]] {destination mask | any | host ip-address} [dscp]
[operator port [port]] [count [byte]] [order] [fragments][log
[interval minutes] [threshold-in-msgs [count]]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no deny udp {source mask | any | host ip-address} {destination mask | any | host ip-address}` command.

Parameters

source	Enter the IP address of the network or host from which the packets were sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword `host` then the IP address to specify a host IP address.
dscp	Enter this keyword `dscp` to deny a packet based on the DSCP value. The range is from 0 to 63.
operator	(OPTIONAL) Enter one of the following logical operand: • `eq` = equal to • `neq` = not equal to • `gt` = greater than • `lt` = less than • `range` = inclusive range of ports (you must specify two ports for the `port` command)
port port	Enter the application layer port number. Enter two port numbers if using the range logical operand. The range is from 0 to 65535.
destination	Enter the IP address of the network or host to which the packets are sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.

byte	(OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.
order	(OPTIONAL) Enter the keyword `order` to specify the QoS priority for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority) If you did not use the keyword `order`, the ACLs have the lowest order by default (**255**).
fragments	Enter the keyword `fragments` to use ACLs to control packet fragments.
log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
threshold-in-msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword then a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs are terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` then the time period in minutes at which the ACL logs must be generated. The time interval range is from 1 to 10 minutes.

Defaults

By default 10 ACL logs are generated if you do not specify the threshold explicitly.

The default frequency at which the ACL logs are generated is five minutes.

Command Modes

CONFIGURATION-IP ACCESS-LIST-EXTENDED

Command History

Version 9.3(0.0)	Added the support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The `order` option is relevant in the context of the Policy QoS feature only. For more information, refer to the Quality of Service chapter of the *Dell Networking OS Configuration Guide*.

In the MXL switch, you can configure either count (packets) or count (bytes). However, for an ACL with multiple rules, you can configure some ACLs with count (packets) and others as count (bytes) at any given time.

Most ACL rules require one entry in the CAM. However, rules with TCP and UDP port operators (for example, gt, lt or range) may require more than one entry. The range of ports is configured in the CAM based on bit mask boundaries; the space required depends on exactly what ports are included in the range.

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that

new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces

Example

An ACL rule with a TCP port range of 4000–8000 uses eight entries in the CAM.

```
Dell#  Data              Mask         From To #Covered

1 0000111110100000 1111111111100000 4000 4031 32
2 0000111111000000 1111111111000000 4032 4095 64
3 0001000000000000 1111100000000000 4096 6143 2048
4 0001100000000000 1111110000000000 6144 7167 1024
5 0001110000000000 1111111000000000 7168 7679 512
6 0001111000000000 1111111100000000 7680 7935 256
7 0001111100000000 1111111111000000 7936 7999 64
8 0001111101000000 1111111111111111 8000 8000 1

Total Ports: 4001
```

Example

An ACL rule with a TCP port lt 1023 uses only one entry in the CAM.

```
Dell# Data              Mask         From To   #Covered

1 0000000000000000 1111110000000000 0    1023 1024

Total Ports: 1024
```

Related Commands

deny — assigns a filter to deny IP traffic.

deny tcp — assigns a filter to deny TCP traffic.

deny arp (for Extended MAC ACLs)

Configure an egress filter that drops ARP packets on egress ACL supported line cards. (For more information, refer to your line card documentation).

Syntax

```
deny arp {destination-mac-address mac-address-mask | any} vlan
vlan-id {ip-address | any | opcode code-number} [count [byte]]
[order] [log [interval minutes] [threshold-in-msgs [count]]
[monitor]
```

To remove this filter, you have two choices:

- Use the `no seq` *sequence-number* command if you know the filter’s sequence number.

- Use the `no deny arp {destination-mac-address mac-address-mask | any} vlan vlan-id {ip-address | any | opcode code-number}` command.

Parameters

destination-mac-address mac-address-mask	Enter a MAC address and mask in the nn:nn:nn:nn:nn format. For the MAC address mask, specify which bits in the MAC address must match. The MAC ACL supports an inverse mask; therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
any	Enter the keyword `any` to match and drop any ARP traffic on the interface. vlan *vlan-id* Enter the keyword `vlan` and then enter the VLAN ID to filter traffic associated with a specific VLAN. The range is 1 to 4094 and 1 to 2094 for ExaScale (you can use IDs 1 to 4094). To filter all VLAN traffic, specify VLAN 1. ip-address Enter an *`IP address`* in dotted decimal format (A.B.C.D) as the target IP address of the ARP. opcode *code-number* Enter the keyword `opcode` and then enter the number of the ARP opcode. The range is from 1 to 23.
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
order	(OPTIONAL) Enter the keyword `order` to specify the QoS priority for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority) If you did not use the keyword order, the ACLs have the lowest order by default (255).
threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation

	of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The time interval range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly.

The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

CONFIGURATION-EXTENDED-ACCESS-LIST

Command History

Version 9.4(0.0)	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platforms.
Version 9.3(0.0)	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module platforms.
Version 8.2.1.0	Allows ACL control of fragmented packets for IP (Layer 3) ACLs.
Version 8.1.1.0	Introduced on the E-Series ExaScale.
Version 7.4.1.0	Added the support for the non-contiguous mask and the `monitor` option.
Version 6.5.1.0	Expanded to include the optional `QoS` order priority for the `ACL` entry.

Usage Information

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

The `order` option is relevant in the context of the Policy QoS feature only. For more information, refer to the Quality of Service chapter of the *Dell Networking OS Configuration Guide*.

The `monitor` option is relevant in the context of flow-based monitoring only. For more information, refer to the Port Monitoring.

When you use the `log` option, the CP processor logs details the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets' details.

You cannot include IP, TCP or UDP (Layer 3) filters in an ACL configured with ARP or Ether-type (Layer 2) filters. Apply Layer 2 ACLs (ARP and Ether-type) to Layer 2 interfaces only.

NOTE: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

deny icmp

To drop all or specific internet control message protocol (ICMP) messages, configure a filter.

Syntax

```
deny icmp {source mask | any | host ip-address} {destination
mask | any | host ip-address} [dscp] [count [byte]] [order]
[fragments][log interval minutes] [threshold-in-msgs] [count]]
[monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command, if you know the filter's sequence number.
- Use the `no deny icmp {source mask | any | host ip-address} {destination mask | any | host ip-address}` command.

Parameters

source	Enter the IP address of the network or host from which the packets were sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.

any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword `host` then the IP address to specify a host IP address.
destination	Enter the IP address of the network or host to which the packets are sent.
dscp	Enter this keyword `dscp` to deny a packet based on the DSCP value. The range is from 0 to 63.
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.
order	(OPTIONAL) Enter the keyword `order` to specify the QoS priority for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority) If you did not use the keyword `order`, the ACLs have the lowest order by default (255).
fragments	Enter the keyword `fragments` to use ACLs to control packet fragments.
log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
threshold-in *msgs count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The time interval range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

CONFIGURATION-IP ACCESS-LIST-EXTENDED

Command History

Version 9.4(0.0)	Added the support for flow-based monitoring on the MXL 10/40GbE Switch IO Module.

Version 9.3(0.0)	Added the support for logging ACLs on the MXL 10/40GbE Switch IO Module.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The `order` option is relevant in the context of the Policy QoS feature only. For more information, refer to the Quality of Service chapter of the *Dell Networking OS Configuration Guide*.

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable`command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

deny ether-type (for Extended MAC ACLs)

Configure an egress filter that drops specified types of Ethernet packets on egress ACL supported line cards. (For more information, refer to your line card documentation).

Syntax

```
deny ether-type protocol-type-number {destination-mac-address
mac-address-mask | any} vlan vlan-id {source-mac-address mac-
address-mask | any} [count [byte]] [order] [log [interval
minutes] [threshold-in-msgs [count]] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq` *`sequence-number`* command if you know the filter's sequence number.

- Use the `no deny ether-type` *`protocol-type-number`* `{`*`destination-mac-address mac-address-mask`* `| any} vlan` *`vlan-id`* `{`*`source-mac-address mac-address-mask`* `| any}` command.

Parameters

protocol-type-number	Enter a number from 600 to FFFF as the specific Ethernet type traffic to drop.
destination-mac-address mac-address-mask	Enter a MAC address and mask in the nn:nn:nn:nn:nn format. For the MAC address mask, specify which bits in the MAC address must match. The MAC ACL supports an inverse mask; therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
any	Enter the keyword `any` to match and drop specific Ethernet traffic on the interface.
vlan *vlan-id*	Enter the keyword `vlan` and then enter the VLAN ID to filter traffic associated with a specific VLAN. The range is 1 to 4094 and 1 to 2094 for ExaScale (you can use IDs 1 to 4094). To filter all VLAN traffic, specify `VLAN 1`.
source-mac-address mac-address-mask	Enter a MAC address and mask in the nn:nn:nn:nn:nn format. For the MAC address mask, specify which bits in the MAC address must match. The MAC ACL supports an inverse mask; therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.
order	(OPTIONAL) Enter the keyword order to specify the QoS priority for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority) If you did not use the keyword `order`, the ACLs have the lowest order by default (255).
log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation

	of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The time interval range is from of 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly.

The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

CONFIGURATION-EXTENDED-ACCESS-LIST

Command History

Version 9.4(0.0)	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platforms.
Version 9.3(0.0)	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module platforms.

Usage Information

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the flow-based `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

deny

To drop packets with a the MAC address specified, configure a filter.

Syntax

```
deny {any | mac-source-address [mac-source-address-mask]}
[count [byte]] [log [interval minutes] [threshold—in-msgs
[count]] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq` *`sequence-number`* command if you know the filter's sequence number.
- Use the `no deny {any |` *`mac-source-address mac-source-address-mask`*`}` command.

Parameters

any	Enter the keyword `any` to specify that all routes are subject to the filter.
mac-source-address	Enter a MAC address in nn:nn:nn:nn:nn:nn format.
mac-source-address-mask	(OPTIONAL) Specify which bits in the MAC address must match. If no mask is specified, a mask of 00:00:00:00:00:00 is applied (in other words, the filter allows only MAC addresses that match).
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword`log` to enable the triggering of ACL log messages.
threshold-in-msgs *count*	(OPTIONAL) Enter the`threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated. with the seq, permit, or deny commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The threshold range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes	CONFIGURATION-MAC ACCESS LIST-STANDARD

Command History

Version 9.4(0.0)	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform.
Version 9.3(0.0)	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module platform.

Usage Information

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

Related Commands

permit — configures a MAC address filter to pass packets.

seq — configures a MAC address filter with a specified sequence number.

deny

To drop packets with a certain IP address, configure a filter.

Syntax

```
deny {any | host mac-address | mac-source-address mac-source-
address-mask}{any | host mac-address | mac-destination-address
mac-destination-address-mask}[ethertype-operator] [count
```

```
[byte]][log [interval minutes] [threshold-in-msgs [count]]
[monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no deny {any | host mac-address | mac-source-address mac-source-address-mask}{any | host mac-address | mac-destination-address mac-destination-address-mask}command.` command.

Parameters

source	Enter the IP address in dotted decimal format of the network from which the packet was sent.
mask	(OPTIONAL) Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous (discontiguous).
any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword `host` and then enter the IP address to specify a host IP address only.
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
threshold-in msgs count	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval minutes	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The time interval range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated, if you do not specify the threshold explicitly.

The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes	CONFIGURATION-IP ACCESS-LIST-STANDARD

Command History

Version 9.4(0.0)	Added the support for flow-based monitoring on the MXL 10/40GbE Switch IO Module.
Version 9.3(0.0)	Added the support for logging of ACLs on the MXL 10/40GbE Switch IO Module.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The `order` option is relevant in the context of the Policy QoS feature only. For more information, refer to the Quality of Service chapter of the *Dell Networking OS Configuration Guide*.

In the MXL switch, you can configure either count (packets) or count (bytes). However, for an ACL with multiple rules, you can configure some ACLs with count (packets) and others as count (bytes) at any given time.

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and s MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only the specified traffic instead of all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

Related Commands

ip access-list standard— configures a standard ACL.

permit — configures a MAC address filter to pass packets.

seq — configures a MAC address filter with a specified sequence number.

permit (for Standard IP ACLs)

To permit packets from a specific source IP address to leave the switch, configure a filter.

Syntax

```
permit {source [mask]| any | host ip-address} [count [byte]]
[dscp value] [order] [fragments] [log [interval minutes]
[threshold-in-msgs [count]] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no permit {source [mask] | any | host ip-address}` command.

Parameters

source	Enter the IP address in dotted decimal format of the network from which the packet was sent.
mask	(OPTIONAL) Enter a network `mask` in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword `host` then the IP address to specify a host IP address or hostname.
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
bytes	(OPTIONAL) Enter the keyword `bytes` to count bytes processed by the filter.
dscp	(OPTIONAL) Enter the keyword `dcsp` to match to the IP DCSCP values.
order	(OPTIONAL) Enter the keyword `order` to specify the QoS priority for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). If you do not use the keyword `order`, the ACLs have the lowest order by default (**255**).
fragments	Enter the keyword `fragments` to use ACLs to control packet fragments.
log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.

interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly.

The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

CONFIGURATION-STANDARD-ACCESS-LIST

Command History

Version 9.4(0.0)	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platforms.
Version 9.3(0.0)	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module platforms.

Usage Information

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

Related Commands

deny — assigns a IP ACL filter to deny IP packets.

ip access-list standard — creates a standard ACL.

permit arp

Configure a filter that forwards ARP packets meeting this criteria. This command is supported only on 12-port GE line cards with SFP optics; refer to your line card documentation for specifications.

Syntax

```
permit arp {destination-mac-address mac-address-mask | any}
vlan vlan-id {ip-address | any | opcode code-number} [count
[byte] | log] [order] [monitor] [fragments] [log [inteval
minutes] [threshold-in-msgs [count]] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `{destination-mac-address mac-address-mask | any} vlan vlan-id {ip-address | any | opcode code-number}` command.

Parameters

destination-mac-address mac-address-mask	Enter a MAC address and mask in the nn:nn:nn:nn:nn format. For the MAC address mask, specify which bits in the MAC address must match. The MAC ACL supports an inverse mask; therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
any	Enter the keyword `any` to match and drop specific Ethernet traffic on the interface.
vlan *vlan-id*	Enter the keyword `vlan` and then enter the VLAN ID to filter traffic associated with a specific VLAN. The range is 1 to 4094 and 1 to 2094 for ExaScale (you can use IDs 1 to 4094). To filter all VLAN traffic, specify `VLAN 1`.
ip-address	Enter an IP address in dotted decimal format (A.B.C.D) as the target IP address of the ARP.
opcode *code-number*	Enter the keyword `opcode` followed by the number of the ARP opcode. The range is 1 to 16.
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.
log	(OPTIONAL, E-Series only) Enter the keyword `log` to have the information kept in an ACL log file.
order	(OPTIONAL) Enter the keyword `order` to specify the QoS priority for the ACL entry. The range is 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority). If you do not use the keyword `order`, the ACLs have the lowest order by default (255).

monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. **NOTE:** For more information, refer to the Flow-based Monitoring section in the Port Monitoring chapter of the *Dell Networking OS Configuration Guide*.
fragments	Enter the keyword `fragments` to use ACLs to control packet fragments.
log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

CONFIGURATION-EXTENDED-ACCESS-LIST

Command History

Version 9.4(0.0)	Added the support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform.
Version 9.3(0.0)	Added the support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.
Version 8.2.1.0	Allows ACL control of fragmented packets for IP (Layer 3) ACLs.
Version 8.1.1.0	Introduced on the E-Series ExaScale.
Version 7.4.1.0	Added the `monitor` option.
Version 6.5.10	Expanded to include the optional QoS `order` priority for the ACL entry.

Usage Information

The `order` option is relevant in the context of the Policy QoS feature only. For more information, refer to the “Quality of Service” chapter of the *Dell Networking OS Configuration Guide*.

When you use the `log` option, the CP processor logs details about the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets’ details.

The `monitor` option is relevant in the context of flow-based monitoring only. For more information, refer to Port Monitoring.

You cannot include IP, TCP, or UDP filters in an ACL configured with ARP filters.

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

NOTE: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

permit ether-type (for Extended MAC ACLs)

Configure a filter that allows traffic with specified types of Ethernet packets. This command is supported only on 12-port GE line cards with SFP optics. For specifications, refer to your line card documentation.

Syntax

```
permit ether-type protocol-type-number {destination-mac-address
mac-address-mask | any} vlan vlan-id {source-mac-address mac-
address-mask | any} [count [byte]] [order] [log
[intervalminutes][threshold-in-msgs] [count]][monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no permit ether-type protocol-type-number {destination-mac-address mac-address-mask | any} vlan vlan-id {source-mac-address mac-address-mask | any}` command.

Parameters

protocol-type-number	Enter a number from 600 to FFF as the specific Ethernet type traffic to drop.
destination-mac-address mac-address-mask	Enter a MAC address and mask in the nn:nn:nn:nn:nn format. For the MAC address mask, specify which bits in the MAC address must match. The MAC ACL supports an inverse mask; therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
any	Enter the keyword `any` to match and drop specific Ethernet traffic on the interface.
vlan *vlan-id*	Enter the keyword `vlan` and then enter the VLAN ID to filter traffic associated with a specific VLAN. The range is 1 to 4094 and 1 to 2094 for ExaScale (you can use IDs 1 to 4094). To filter all VLAN traffic specify `VLAN 1`.
source-mac-address mac-address-mask	Enter a MAC address and mask in the nn:nn:nn:nn:nn format. For the MAC address mask, specify which bits in the MAC address must match. The MAC ACL supports an inverse mask; therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.
order	(OPTIONAL) Enter the keyword `order` to specify the QoS priority for the ACL entry. The range is 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority). If you do not use the keyword `order`, the ACLs have the lowest order by default (255).

log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. You can enter an interval in the range of 1-10 minutes.
threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated. with the seq, permit, or deny commands. The threshold range is from 1 to 100.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. NOTE: For more information, refer to the Flow-based Monitoring section in the Port Monitoring chapter of the *Dell Networking OS Configuration Guide*.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

CONFIGURATION-EXTENDED-ACCESS-LIST

Command History

Version 9.4(0.0)	Added the support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform.
Version 9.3(0.0)	Added the support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.
Version 8.2.1.0	Allows ACL control of fragmented packets for IP (Layer 3) ACLs.
Version 8.1.1.0	Introduced on the E-Series ExaScale.
Version 7.4.1.0	Added the `monitor` option.
Version 6.5.10	Expanded to include the optional QoS `order` priority for the ACL entry.

Usage Information

The `order` option is relevant in the context of the Policy QoS feature only. For more information, refer to the “Quality of Service” chapter of the *Dell Networking OS Configuration Guide*.

NOTE: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

When you use the `log` option, the CP processor logs details about the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets' details.

The `monitor` option is relevant in the context of flow-based monitoring only. For more information, refer to Port Monitoring.

You cannot include IP, TCP, or UDP filters in an ACL configured with ARP filters.

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

permit icmp

Configure a filter to allow all or specific ICMP messages.

Syntax

```
permit icmp {source mask | any | host ip-address} {destination
mask | any | host ip-address} [dscp] [message-type] [count
[byte]] [order] [fragments][log [interval minutes] [threshold-
in-msgs [count]] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no permit icmp {source mask | any | host ip-address} {destination mask | any | host ip-address}` command.

Parameters

source	Enter the IP address of the network or host from which the packets were sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or noncontiguous.
any	Enter the keyword `any` to match and drop specific Ethernet traffic on the interface.
host *ip-address*	Enter the keyword `host` and then enter the IP address to specify a host IP address.
destination	Enter the IP address of the network or host to which the packets are sent.
dscp	Enter the keyword `dscp` to deny a packet based on the DSCP value. The range is 0 to 63.
message-type	(OPTIONAL) Enter an ICMP message type, either with the type (and code, if necessary) numbers or with the name of the message type. The range is 0 to 255 for ICMP type and 0 to 255 for ICMP code.
count	(OPTIONAL) Enter the keyword `count` to count packets the filter processes.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes the filter processes.
order	(OPTIONAL) Enter the keyword `order` to specify the QoS priority for the ACL entry. The range is 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). If you do not use the keyword `order`, the ACLs have the lowest order by default (**255**).
fragments	Enter the keyword `fragments` to use ACLs to control packet fragments.
log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL

in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

CONFIGURATION-IP ACCESS-LIST-STANDARD

Command History

Version 9.4(0.0)	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform.
Version 9.3(0.0)	Added the support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The `order` option is relevant in the context of the Policy QoS feature only. For more information, refer to the Quality of Service chapter of the *Dell Networking OS Configuration Guide*.

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

permit udp

To pass UDP packets meeting the filter criteria, configure a filter.

Syntax

`permit udp {source mask | any | host ip-address} [operator port [port]] {destination mask | any | host ip-address} [dscp] [operator port [port]] [count [byte]] [order] [fragments] [log [interval minutes] [threshold-in-msgs [count]] [monitor]`

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no permit udp {source mask | any | host ip-address} {destination mask | any | host ip-address` command.

Parameters

source	Enter the IP address of the network or host from which the packets were sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword `host` and then enter the IP address to specify a host IP address.
dscp	Enter the keyword `dscp` to deny a packet based on the DSCP value. The range is from 0 to 63.
operator	(OPTIONAL) Enter one of the following logical operand: • `eq` = equal to • `neq` = not equal to • `gt` = greater than • `lt` = less than • `range` = inclusive range of ports (you must specify two ports for the `port` parameter)
port port	Enter the application layer port number. Enter two port numbers if you are using the `range` logical operand. The range is 0 to 65535.
destination	Enter the IP address of the network or host to which the packets are sent.
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.
order	(OPTIONAL) Enter the keyword `order` to specify the QoS priority for the ACL entry. The range is from 0 to 254 (where

	0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). If you do not use the keyword `order`, the ACLs have the lowest order by default (**255**).
fragments	Enter the keyword `fragments` to use ACLs to control packet fragments.
log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

CONFIGURATION-IP ACCESS-LIST-EXTENDED

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The `order` option is relevant in the context of the Policy QoS feature only. For more information, refer to the “Quality of Service” chapter of the *Dell Operating System Configuration Guide*.

In the MXL switch, you can configure either count (packets) or count (bytes). However, for an ACL with multiple rules, you can configure some ACLs with count (packets) and others as count (bytes) at any given time.

Most ACL rules require one entry in the CAM. However, rules with TCP and UDP port operators (for example, gt, lt, or range) may require more than one entry. The range of ports is configured in the CAM based on bit mask boundaries; the space required depends on exactly what ports are included in the range.

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that

new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

Example

An ACL rule with a TCP port range of 4000–8000 uses eight entries in the CAM.

```
Dell# Data             Mask         From To   #Covered

1 0000111110100000 1111111111100000 4000 4031 32
2 0000111111000000 1111111111000000 4032 4095 64
3 0001000000000000 1111100000000000 4096 6143 2048
4 0001100000000000 1111110000000000 6144 7167 1024
5 0001110000000000 1111111000000000 7168 7679 512
6 0001111000000000 1111111100000000 7680 7935 256
7 0001111100000000 1111111111000000 7936 7999 64
8 0001111101000000 1111111111111111 8000 8000 1

Total Ports: 4001
```

Example

An ACL rule with a TCP port lt 1023 uses only one entry in the CAM.

```
Dell# Data            Mask          From To   #Covered

1 0000000000000000 1111110000000000 0    1023 1024

Total Ports: 1024
```

Related Commands

ip access-list extended — creates an extended ACL.

permit — assigns a permit filter for IP packets.

permit tcp — assigns a permit filter for TCP packets.

permit (for Extended IP ACLs)

To pass IP packets meeting the filter criteria, configure a filter.

Syntax

```
permit {source mask | any | host ip-address} {destination mask
| any | host ip-address} [count [bytes]] [dscp value] [order]
[fragments] [log [interval minutes] [threshold-in-msgs [count]]
[monitor]
```

To remove this filter, you have two choices:

- Use the `no seq` *`sequence-number`* command if you know the filter's sequence number.
- Use the `no deny {`*`source mask`*` | any | host `*`ip-address`*`} {`*`destination mask`*` | any | host `*`ip-address`*`}` command.

Parameters

source	Enter the IP address in dotted decimal format of the network from which the packet was sent.
mask	(OPTIONAL) Enter a network `mask` in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword `host` then the IP address to specify a host IP address or hostname.
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
bytes	(OPTIONAL) Enter the keyword `bytes` to count bytes processed by the filter.
dscp	(OPTIONAL) Enter the keyword `dcsp` to match to the IP DCSCP values.
order	(OPTIONAL) Enter the keyword order to specify the QoS priority for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). If you do not use the keyword `order`, the ACLs have the lowest order by default (**255**).
fragments	Enter the keyword `fragments` to use ACLs to control packet fragments.
log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.

interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly.

The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

CONFIGURATION-EXTENDED-ACCESS-LIST

Command History

Version 9.4(0.0)	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platforms.
Version 9.3(0.0)	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.

Usage Information

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

Related Commands

ip access-list extended — creates an extended ACL.

permit tcp — assigns a permit filter for TCP packets.

permit udp — assigns a permit filter for UDP packets.

permit

To forward packets from a specific source MAC address, configure a filter.

Syntax

```
permit {any | mac-source-address [mac-source-address-mask]}
[count [byte]] | log [interval minutes] [threshold-in-
msgs[count] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no permit {any | mac-source-address mac-source-address-mask}` command.

Parameters

any	Enter the keyword `any` to forward all packets received with a MAC address.
mac-source-address	Enter a MAC address in nn:nn:nn:nn:nn:nn format.
mac-source-address-mask	(OPTIONAL) Specify which bits in the MAC address must match. If no mask is specified, a mask of 00:00:00:00:00:00 is applied (in other words, the filter allows only MAC addresses that match).
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface

Defaults	Not configured.
Command Modes	CONFIGURATION-MAC ACCESS LIST-STANDARD

Command History

Version 9.4(0.0)	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform.
Version 9.3(0.0)	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

When the configured maximum threshold is exceeded, generation of logs are stopped.

When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, Pv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

Related Commands

deny — configures a MAC ACL filter to drop packets.

seq —configure a MAC ACL filter with a specified sequence number.

seq

To a deny or permit filter in a MAC access list while creating the filter, assign a sequence number.

Syntax

```
seq sequence-number {deny | permit} {any | mac-source-address
[mac-source-address-mask]} [count [byte]] [log [interval
minutes] [threshold-in-msgs [count]] [monitor]
```

To remove this filter, use the `no seq sequence-number` command.

Parameters

sequence-number	Enter a number from 0 to 65535.
deny	Enter the keyword `deny` to configure a filter to drop packets meeting this condition.
permit	Enter the keyword `permit` to configure a filter to forward packets meeting this criteria.
any	Enter the keyword `any` to filter all packets.
mac-source-address	Enter a MAC address in nn:nn:nn:nn:nn:nn format.
mac-source-address-mask	(OPTIONAL) Specify which bits in the MAC address must match. If no mask is specified, a mask of 00:00:00:00:00:00 is applied (in other words, the filter allows only MAC addresses that match).
count	(OPTIONAL) Enter the keyword `count` to count packets the filter processes.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes the filter processes.
log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes..
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

CONFIGURATION-MAC ACCESS LIST-STANDARD

Command History

Version 9.4(0.0)	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform.
Version 9.3(0.0)	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

Related Commands

deny — configures a filter to drop packets.

permit — configures a filter to forward packets.

permit tcp

To pass TCP packets meeting the filter criteria, configure a filter.

Syntax

```
permit tcp {source mask | any | host ip-address} [bit]
[operator port [port]] {destination mask | any | host ip-
address} [bit] [dscp] [operator port [port]] [count [byte]]
[order] [fragments][log [interval minutes] [threshold-in-msgs
[count]] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no permit tcp {source mask | any | host ip-address} {destination mask | any | host ip-address}` command.

Parameters

source	Enter the IP address of the network or host from which the packets were sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword `host` then the IP address to specify a host IP address.
bit	Enter a flag or combination of bits: • `ack`: acknowledgement field • `fin`: finish (no more data from the user) • `psh`: push function • `rst`: reset the connection • `syn`: synchronize sequence numbers • `urg`: urgent field
dscp	Enter the keyword `dscp` to deny a packet based on the DSCP value. The range is from 0 to 63.
operator	(OPTIONAL) Enter one of the following logical operand: • `eq` = equal to • `neq` = not equal to • `gt` = greater than • `lt` = less than • `range` = inclusive range of ports (you must specify two ports for the port parameter)

port port	Enter the application layer port number. Enter two port numbers if you are using the range logical operand. The range is from 0 to 65535. The following list includes some common TCP port numbers: • 23 = Telnet • 20 and 21 = FTP • 25 = SMTP • 169 = SNMP
destination	Enter the IP address of the network or host to which the packets are sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
count	(OPTIONAL) Enter the keyword `count` to count packets the filter processes.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes the filter processes.
order	(OPTIONAL) Enter the keyword `order` to specify the QoS priority for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). If you do not use the keyword `order`, the ACLs have the lowest order by default (**255**).
fragments	Enter the keyword `fragments` to use ACLs to control packet fragments.
log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or deny commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The threshold range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

CONFIGURATION-IP ACCESS-LIST-EXTENDED

Command History

Version 9.4(0.0)	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform.
Version 9.3(0.0)	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module platform.

Usage Information

The `order` option is relevant in the context of the Policy QoS feature only. For more information, refer to the "Quality of Service" chapter of the *Dell Networking OS Configuration Guide*.

The MXL 10/40GbE System IO Module cannot count both packets and bytes, so when you enter the count byte options, only bytes are incremented.

Most ACL rules require one entry in the CAM. However, rules with TCP and UDP port operators (for example, gt, lt, or range) may require more than one entry. The range of ports is configured in the CAM based on bit mask boundaries; the space required depends on exactly what ports are included in the range.

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

Example

An ACL rule with a TCP port range of 4000–8000 uses eight entries in the CAM.

```
Dell# Data              Mask          From To   #Covered

1 0000111110100000 1111111111100000 4000 4031 32
2 0000111111000000 1111111111000000 4032 4095 64
3 0001000000000000 1111100000000000 4096 6143 2048
4 0001100000000000 1111110000000000 6144 7167 1024
5 0001110000000000 1111111000000000 7168 7679 512
6 0001111000000000 1111111100000000 7680 7935 256
7 0001111100000000 1111111111000000 7936 7999 64
8 0001111101000000 1111111111111111 8000 8000 1

Total Ports: 4001
```

Example

An ACL rule with a TCP port lt 1023 uses only one entry in the CAM.

```
Dell# Data             Mask           From To   #Covered

1 0000000000000000 1111110000000000 0    1023 1024

Total Ports: 1024
```

Related Commands

ip access-list extended — creates an extended ACL.

permit — assigns a permit filter for IP packets.

permit udp — assigns a permit filter for UDP packets.

seq arp

Configure an egress filter with a sequence number that filters ARP packets meeting this criteria. This command is supported only on 12-port GE line cards with SFP optics. For specifications, refer to your line card documentation.

Syntax

```
seq sequence-number {deny | permit} arp {destination-mac-
address mac-address-mask | any} vlan vlan-id {ip-address | any
| opcode code-number} [count [byte] [order] [log [interval
minutes] [threshold-in-msgs[count]] [monitor]
```

To remove this filter, use the no seq *sequence-number* command.

Parameters

sequence-number	Enter a number from 0 to 4294967290.
deny	Enter the keyword `deny` to drop all traffic meeting the filter criteria..
permit	Enter the keyword `permit` to forward all traffic meeting the filter criteria.

destination-mac-address mac-address-mask	Enter a MAC address and mask in the nn:nn:nn:nn:nn format. For the MAC address mask, specify which bits in the MAC address must match. The MAC ACL supports an inverse mask; therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
any	Enter the keyword `any` to match and drop any ARP traffic on the interface.
vlan *vlan-id*	Enter the keyword `vlan` followed by the VLAN ID to filter traffic associated with a specific VLAN. The range is 1 to 4094 and 1 to 2094 for ExaScale (you can use IDs 1 to 4094). To filter all VLAN traffic specify `VLAN 1`.
ip-address	Enter an IP address in dotted decimal format (A.B.C.D) as the target IP address of the ARP.
opcode *code-number*	Enter the keyword `opcode` and then enter the number of the ARP opcode. The range is 1 to 16.
count	(OPTIONAL) Enter the keyword `count` to count packets the filter processes.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes the filter processes.
order	(OPTIONAL) Enter the keyword `order` to specify the QoS priority for the ACL entry. The range is 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). If you do not use the keyword `order`, the ACLs have the lowest order by default (255).
log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.
threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

NOTE: For more information, refer to the Flow-based Monitoring section in the Port Monitoring chapter of the *Dell Networking OS Configuration Guide*.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

CONFIGURATION-EXTENDED-ACCESS-LIST

Command History

Version 9.4(0.0)	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform.
Version 9.3(0.0)	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.
Version 8.2.1.0	Allows ACL control of fragmented packets for IP (Layer 3) ACLs.
Version 8.1.1.0	Introduced on the E-Series ExaScale.
Version 7.4.1.0	Added the `monitor` option.
Version 6.5.10	Expanded to include the optional QoS `order` priority for the ACL entry.

Usage Information

The `monitor` option is relevant in the context of flow-based monitoring only. For more information, refer to Port Monitoring.

The `order` option is relevant in the context of the Policy QoS feature only. The following applies:

- The `seq` *`sequence-number`* command is applicable only in an ACL group.
- The `order` option works across ACL groups that have been applied on an interface via the QoS policy framework.
- The `order` option takes precedence over `seq` *`sequence-number`*.
- If *`sequence-number`* is not configured, the rules with the same order value are ordered according to their configuration order.
- If *`sequence-number`* is configured, the sequence-number is used as a tie breaker for rules with the same order.

When you use the `log` option, the CP processor logs details about the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets' details.

You cannot include IP, TCP, or UDP (Layer 3) filters in an ACL configured with ARP or Ether-type (Layer 2) filters. Apply Layer 2 ACLs to interfaces in Layer 2 mode.

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that

new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

NOTE: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

seq ether-type

Configure an egress filter with a specific sequence number that filters traffic with specified types of Ethernet packets. This command is supported only on 12-port GE line cards with SFP optics. For specifications, refer to your line card documentation.

Syntax

```
seq sequence-number {deny | permit} ether-type protocol-type-
number {destination-mac-address mac-address-mask | any} vlan
vlan-id {source-mac-address mac-address-mask | any} [count
[byte] [order] [log [interval minutes] [threshold-in-msgs
[count]] [monitor]
```

To remove this filter, use the no seq *sequence-number* command.

Parameters

sequence-number	Enter a number from 0 to 4294967290.
deny	Enter the keyword `deny` to drop all traffic meeting the filter criteria..
permit	Enter the keyword `permit` to forward all traffic meeting the filter criteria.

destination-mac-address mac-address-mask	Enter a MAC address and mask in the nn:nn:nn:nn:nn format. For the MAC address mask, specify which bits in the MAC address must match. The MAC ACL supports an inverse mask; therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
any	Enter the keyword `any` to match and drop specific Ethernet traffic on the interface.
vlan *vlan-id*	Enter the keyword `vlan` and then enter the VLAN ID to filter traffic associated with a specific VLAN. The range is 1 to 4094 and 1 to 2094 for ExaScale (you can use IDs 1 to 4094). To filter all VLAN traffic specify `VLAN 1`.
source-mac-address mac-address-mask	Enter a MAC address and mask in the nn:nn:nn:nn:nn format. For the MAC address mask, specify which bits in the MAC address must match. The MAC ACL supports an inverse mask; therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
count	(OPTIONAL) Enter the keyword `count` to count packets the filter processes.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes the filter processes.
order	(OPTIONAL) Enter the keyword `order` to specify the QoS priority for the ACL entry. The range is 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). If you do not use the keyword `order`, the ACLs have the lowest order by default (255).
log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.
threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.

monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. **NOTE:** For more information, refer to the Flow-based Monitoring section in the Port Monitoring chapter of the *Dell Networking OS Configuration Guide*.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

CONFIGURATION-EXTENDED-ACCESS-LIST

Command History

Version 9.4(0.0)	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform.
Version 9.3(0.0)	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.
Version 8.2.1.0	Allows ACL control of fragmented packets for IP (Layer 3) ACLs.
Version 8.1.1.0	Introduced on the E-Series ExaScale.
Version 7.4.1.0	Added the `monitor` option.
Version 6.5.10	Expanded to include the optional QoS `order` priority for the ACL entry.

Usage Information

The `monitor` option is relevant in the context of flow-based monitoring only. For more information, refer to Port Monitoring.

The `order` option is relevant in the context of the Policy QoS feature only. The following applies:

- The `seq` *`sequence-number`* command is applicable only in an ACL group.
- The `order` option works across ACL groups that have been applied on an interface via the QoS policy framework.
- The `order` option takes precedence over `seq` *`sequence-number`*.
- If *`sequence-number`* is not configured, the rules with the same order value are ordered according to their configuration order.
- If *`sequence-number`* is configured, the sequence-number is used as a tie breaker for rules with the same order.

When you use the `log` option, the CP processor logs details about the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets’ details.

You cannot include IP, TCP, or UDP (Layer 3) filters in an ACL configured with ARP or Ether-type (Layer 2) filters. Apply Layer 2 ACLs to interfaces in Layer 2 mode.

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

NOTE: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

seq

Assign a sequence number to a deny or permit filter in an extended IP access list while creating the filter.

Syntax

```
seq sequence-number {deny | permit} {source [mask] | any | host
ip-address}} [count [byte] [dscp value] [order] [fragments]
[log [interval minutes] [threshold-in-msgs [count] [monitor]
```

Parameters

sequence-number	Enter a number from 0 to 4294967290. The range is from 0 to 65534.
deny	Enter the keyword `deny` to configure a filter to drop packets meeting this condition.
permit	Enter the keyword `permit` to configure a filter to forward packets meeting this criteria.
source	Enter an IP address in dotted decimal format of the network from which the packet was received.

mask	(OPTIONAL) Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword `any` to specify that all routes are subject to the filter.
count	(OPTIONAL) Enter the keyword `count` to count packets the filter processes.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes the filter processes.
dscp	(OPTIONAL) Enter the keyword `dcsp` to match to the IP DCSCP values.
order	(OPTIONAL) Enter the keyword `order` to specify the QoS order for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). If you do not use the keyword `order`, the ACLs have the lowest order by default (**255**).
fragments	Enter the keyword `fragments` to use ACLs to control packet fragments.
log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
threshold-in *msgs* count	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` then by the time period in minutes at which the ACL logs must be generated. The interval range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

CONFIGURATION-IP ACCESS-LIST-STANDARD

Command History

Version 9.4(0.0)	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform.

Version 9.3(0.0)	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The `order` option is relevant in the context of the Policy QoS feature only. The following applies:

- The `seq` *`sequence-number`* command is applicable only in an ACL group.
- The `order` option works across ACL groups that have been applied on an interface via the QoS policy framework.
- The `order` option takes precedence over `seq` *`sequence-number`*.
- If *`sequence-number`* is not configured, the rules with the same order value are ordered according to their configuration order.
- If *`sequence-number`* is configured, the sequence-number is used as a tie breaker for rules with the same order.

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

Related Commands

deny — configures a filter to drop packets.

permit — configures a filter to forward packets.

seq — assigns a sequence number to a deny or permit filter in an IP access list while creating the filter.

seq

Assign a sequence number to a deny or permit filter in an extended IP access list while creating the filter.

Syntax

```
seq sequence-number {deny | permit} {ipv6-protocol-number |
icmp | ip | tcp | udp} {source mask | any | host ipv6-address}
{destination mask | any | host ipv6-address} [operator port
[port]] [count [byte]] [dscp value] [order] [fragments] [log
[interval minutes] [threshold-in-msgs [count]] [monitor]
```

Parameters

sequence-number	Enter a number from 0 to 4294967290. The range is from 1 to 65534.
deny	Enter the keyword `deny` to configure a filter to drop packets meeting this condition.
permit	Enter the keyword `permit` to configure a filter to forward packets meeting this criteria.
ipv6-protocol-number	Enter a number from 0 to 255 to filter based on the protocol identified in the IP protocol header.
icmp	Enter the keyword `icmp` to configure an ICMP access list filter.
ip	Enter the keyword `ip` to configure a generic IP access list. The keyword `ip` specifies that the access list permits all IP protocols.
tcp	Enter the keyword `tcp` to configure a TCP access list filter.
udp	Enter the keyword `udp` to configure a UDP access list filter.
source	Enter an IP address in dotted decimal format of the network from which the packet was received.
mask	(OPTIONAL) Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ipv6-address*	Enter the keyword `host` and then enter the IPv6 address to specify a host IP address or hostname.
operator	(OPTIONAL) Enter one of the following logical operands: • `eq` = equal to • `neq` = not equal to • `gt` = greater than • `lt` = less than • `range` = inclusive range of ports (you must specify two ports for the `port` parameter.)

port port	(OPTIONAL) Enter the application layer port number. Enter two port numbers if you are using the range logical operand. The range is from 0 to 65535. The following list includes some common TCP port numbers: • 23 = Telnet • 20 and 21 = FTP • 25 = SMTP • 169 = SNMP
destination	Enter the IP address of the network or host to which the packets are sent.
count	(OPTIONAL) Enter the keyword `count` to count packets the filter processes.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes the filter processes.
dscp	(OPTIONAL) Enter the keyword `dcsp` to match to the IP DCSCP values.
order	(OPTIONAL) Enter the keyword `order` to specify the QoS order for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). If you do not use the keyword `order`, the ACLs have the lowest order by default (**255**).
fragments	Enter the keyword `fragments` to use ACLs to control packet fragments.
log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
threshold-in msgs count	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval minutes	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which the ACL logs must be generated. The interval range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which the ACL logs are generated is five minutes. By default, the flow-based monitoring is not enabled.

Command Modes	ACCESS-LIST

Command History

Version 9.4(0.0)	Added support for the flow-based monitoring on the MXL 10/40GbE Switch IO Module.
Version 9.3(0.0)	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The `order` option is relevant in the context of the Policy QoS feature only. The following applies:

- The `seq` *`sequence-number`* command is applicable only in an ACL group.
- The `order` option works across ACL groups that have been applied on an interface via the QoS policy framework.
- The `order` option takes precedence over `seq` *`sequence-number`*.
- If *`sequence-number`* is not configured, the rules with the same order value are ordered according to their configuration order.
- If *`sequence-number`* is configured, the sequence-number is used as a tie breaker for rules with the same order.

If you configure the *`sequence-number`*, the *`sequence-number`* is used as a tie breaker for rules with the same order.

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

Related Commands

deny — Configures a filter to drop packets.

permit — Configures a filter to forward packets.

permit udp

Configure a filter to pass UDP packets meeting the filter criteria.

Syntax

```
permit udp {source address mask | any | host ipv6-address}
[operator port [port]] {destination address | any | host ipv6-
address} [operator port [port]] [count [byte]] [log [interval
minutes] [threshold-in-msgs [count]][monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no permit udp {source address mask | any | host ipv6-address} {destination address | any | host ipv6-address}` command.

Parameters

source address	Enter the IPv6 address of the network or host from which the packets were sent in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128. The :: notation specifies successive hexadecimal fields of zero.
mask	Enter a network mask in /prefix format (/x).
any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ipv6-address*	Enter the keyword `host` followed by the IPv6 address of the host in the x:x:x:x::x format. The :: notation specifies successive hexadecimal fields of zero.
operator	(OPTIONAL) Enter one of the following logical operand: • `eq` = equal to • `neq` = not equal to • `gt` = greater than • `lt` = less than • `range` = inclusive range of ports (you must specify two port for the port parameter.)
port port	(OPTIONAL) Enter the application layer port number. Enter two port numbers if using the range logical operand. The range is 0 to 65535.

destination address	Enter the IPv6 address of the network or host to which the packets are sent in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128. The :: notation specifies successive hexadecimal fields of zero.
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which the ACL logs are generated in five minutes. By default, flow-based monitoring is not enabled.

Command Modes

ACCESS-LIST

Command History

Version 9.4(0.0)	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform.
Version 9.3(0.0)	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.

Usage Information

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces. you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

Related Commands

permit – assigns a permit filter for IP packets.

permit tcp – assigns a permit filter for TCP packets.

permit tcp

Configure a filter to pass TCP packets that match the filter criteria.

Syntax

```
permit tcp {source address mask | any | host ipv6-address}
[operator port [port]] {destination address | any | host ipv6-
address} [bit] [operator port [port]] [count [byte]] [log
[interval minutes] [threshold-in-msgs [count][monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no permit tcp {source address mask | any | host ipv6-address} {destination address | any | host ipv6-address}` command.

Parameters

source address	Enter the IPv6 address of the network or host from which the packets were sent in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128. The :: notation specifies successive hexadecimal fields of zero.
mask	Enter a network mask in /prefix format (/x).
any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ipv6-address*	Enter the keyword `host` followed by the IPv6 address of the host in the x:x:x:x::x format. The :: notation specifies successive hexadecimal fields of zero.

operator	(OPTIONAL) Enter one of the following logical operand: • `eq` = equal to • `neq` = not equal to • `gt` = greater than • `lt` = less than • `range` = inclusive range of ports (you must specify two port for the port parameter.)
port port	Enter the application layer port number. Enter two port numbers if using the range logical operand. The range is 0 to 65535. The following list includes some common TCP port numbers: • 23 = Telnet • 20 and 21 = FTP • 25 = SMTP • 169 = SNMP
destination address	Enter the IPv6 address of the network or host to which the packets are sent in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128. The :: notation specifies successive hexadecimal fields of zero.
bit	Enter a flag or combination of bits: • `ack:` acknowledgement field • `fin:` finish (no more data from the user) • `psh:` push function • `rst:` reset the connection • `syn:` synchronize sequence numbers • `urg:` urgent field
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.

interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

ACCESS-LIST

Command History

Version 9.4(0.0)	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform.
Version 9.3(0.0)	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.

Usage Information

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

Related Commands

permit – assigns a permit filter for IP packets.

permit udp – assigns a permit filter for UDP packets.

permit icmp

To allow all or specific internet control message protocol (ICMP) messages, configure a filter.

Syntax

```
permit icmp {source address mask | any | host ipv6-address}
{destination address | any | host ipv6-address} [message-type]
[count [byte]] | [log] [interval minutes] [threshold-in-msgs
[count]][monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no permit icmp {source address mask | any | host ipv6-address} {destination address | any | host ipv6-address}` command.

Parameters

source address	Enter the IPv6 address of the network or host from which the packets were sent in the x:x:x:x::x format then the prefix length in the /x format. The range is from /0 to /128. The :: notation specifies successive hexadecimal fields of zero.
mask	Enter a network mask in /prefix format (/x).
any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ipv6-address*	Enter the keyword `host` then the IPv6 address of the host in the x:x:x:x::x format. The :: notation specifies successive hexadecimal fields of zero.
destination address	Enter the IPv6 address of the network or host to which the packets are sent in the x:x:x:x::x format then the prefix length in the /x format. The range is from /0 to /128. The :: notation specifies successive hexadecimal fields of zero.
message-type	(OPTIONAL) Enter an ICMP message type, either with the type (and code, if necessary) numbers or with the name of the message type. The range is from 0 to 255 for ICMP type and from 0 to 255 for ICMP code.
count	(OPTIONAL) Enter the keyword `count` to count packets the filter processes.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes the filter processes.
log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
threshold-in-msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.

interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

ACCESS-LIST

Command History

Version 9.4(0.0)	Added the support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform
Version 9.3(0.0)	Added the support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform
Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module platform.

Usage Information

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

permit

To configure a filter that matches the filter criteria, select an IPv6 protocol number, ICMP, IPv6, TCP, or UDP.

Syntax

```
permit {ipv6-protocol-number | icmp | ipv6 | tcp | udp} [count
[byte]] [dscp value] [order] [fragments] [log [interval
minutes] [threshold-in-msgs [count]] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command syntax if you know the filter's sequence number
- Use the `no permit {ipv6-protocol-number | icmp | ipv6 | tcp | udp}` command

Parameters

ip-protocol-number	Enter an IPv6 protocol number. The range is from 0 to 255.
icmp	Enter the keyword `icmp` to filter internet Control Message Protocol version 6.
ipv6	Enter the keyword `ipv6` to filter any internet Protocol version 6.
tcp	Enter the keyword `tcp` to filter the Transmission Control protocol.
udp	Enter the keyword `udp` to filter the User Datagram Protocol.
count	(OPTIONAL) Enter the keyword `count` to count packets the filter processes.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes the filter processes.
dscp	(OPTIONAL) Enter the keyword `dcsp` to match to the IP DCSCP values.
order	(OPTIONAL) Enter the keyword order to specify the QoS priority for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). If you do not use the keyword `order`, the ACLs have the lowest order by default (**255**).
fragments	Enter the keyword `fragments` to use ACLs to control packet fragments.
log	OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
threshold-in-*msgs*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.

interval *minutes*	(OPTIONAL) Enter the `keyword` interval followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults Not configured.

Command Modes ACCESS-LIST

Command History

Version 9.4(0.0)	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module.
Version 9.3(0.0)	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module.
Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

deny udp (for IPv6 ACLs)

Configure a filter to drop user datagram protocol (UDP) packets meeting the filter criteria.

Syntax

```
deny udp {source address mask | any | host ipv6-address}
[operator port [port]] {destination address | any | host ipv6-
address} [operator port [port]] [count [byte]] [log [interval
minutes] [threshold-in-msgs [count]] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command syntax if you know the filter's sequence number
- Use the `no deny udp {source address mask | any | host ipv6-address} {destination address | any | host ipv6-address}` command

Parameters

source	Enter the IP address of the network or host from which the packets are sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword `any` to specify that all routes are subject to the filter.

host *ipv6–address*	Enter the keyword `host` then the IPv6 address to specify a host IP address.
operator	(OPTIONAL) Enter one of the following logical operand. • eq = equal to • neq = not equal to • gt = greater than • lt = less than • range = inclusive range of ports (you must specify two ports for the `port` command)
port	Enter the application layer port number. Enter two port numbers if using the range logical operand. The range is from 0 to 65535. The following list includes some common TCP port numbers: • 23 = Telnet • 20 and 21 = FTP • 25 = SMTP • 169 = SNMP
count	(OPTIONAL) Enter the keyword `count` to count the packets that filter the processes.
byte	(OPTIONAL) Enter the keyword `byte` to count the bytes that filter the processes.
log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The threshold range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly.

The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes	ACCESS-LIST
Command History	**Version 9.4(0.0)** Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform. **Version 9.3(0.0)** Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.
Usage Information	When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval. If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces. You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).
Related Commands	deny – assigns a filter to deny IP traffic. deny tcp – assigns a deny filter for TCP traffic.

deny tcp (for IPv6 ACLs)

Configure a filter that drops TCP packets that match the filter criteria.

Syntax

```
deny tcp {source address mask | any | host ipv6-address}
[operator port [port]] {destination address | any | host ipv6-
address} [bit] [operator port [port]] [count [byte]] [log
[interval minutes] [threshold-in-msgs [count]] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command syntax if you know the filter's sequence number
- Use the `no deny tcp {`*`source address mask`*` | any | host `*`ipv6-address`*`} {`*`destination address`*` | any | host `*`ipv6-address`*`}` command

Parameters

source	Enter the IP address of the network or host from which the packets are sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ipv6–address*	Enter the keyword `host` then the IPv6 address to specify a host IP address.
operator	(OPTIONAL) Enter one of the following logical operand: • eq = equal to • neq = not equal to • gt = greater than • lt = less than • range = inclusive range of ports (you must specify two ports for the `port` command)
port	Enter the application layer port number. Enter two port numbers if using the range logical operand. The range is from 0 to 65535. The following list includes some common TCP port numbers: • 23 = Telnet • 20 and 21= FTP • 25 = SMTP • 169 = SNMP
destination	Enter the IP address of the network or host to which the packets are sent.
bit	(OPTIONAL) Enter the keyword `bit` to count the bits that filter the processes.
count	(OPTIONAL) Enter the keyword `count` to count the packets that filter the processes.

byte	(OPTIONAL) Enter the keyword `byte` to count the bytes that filter the processes.
log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The time interval range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly.

The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

ACCESS-LIST

Command History

Version 9.4(0.0)	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform.
Version 9.3(0.0)	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.

Usage Information

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the`flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface.

This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

Related Commands

deny – assigns a filter to deny IP traffic.

deny udp – assigns a filter to deny UDP traffic.

deny icmp (for Extended IPv6 ACLs)

Configure a filter to drop all or specific ICMP messages.

Syntax

```
deny icmp {source address mask | any | host ipv6-address}
{destination address | any | host ipv6-address} [count [byte]]
| [log [interval minutes] [threshold-in-msgs [count]] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command syntax if you know the filter's sequence number
- Use the `no deny icmp {source address mask | any | host ipv6-address} {destination address | any | host ipv6-address}` command

Parameters

`

source	Enter the IPv6 address of the network or host from which the packets were sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ipv6–address*	Enter the keyword `host` then the IPv6 address to specify a host IP address.
destination	Enter the IPv6 address of the network or host to which the packets are sent.
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.

threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The time interval range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly.

The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

ACCESS-LIST

Command History

Version 9.4(0.0)	Added the support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform.
Version 9.3(0.0)	Added the support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.

Usage Information

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

deny (for IPv6 ACLs)

Configure a filter that drops IPv6 packets that match the filter criteria.

Syntax

`deny {ipv6-protocol-number | icmp | ipv6 | tcp | udp} [count [byte]] [dscp value] [order] [fragments] [log [interval minutes] [threshold-in-msgs [count]] [monitor]`

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command syntax if you know the filter's sequence number
- Use the `no deny {ipv6-protocol-number | icmp | ipv6 | tcp | udp}` command

Parameters

count	OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.
dscp	(OPTIONAL) Enter the keyword `dscp` to match to the IP DSCP values.
order	(OPTIONAL) Enter the keyword `order` to specify the QoS order of priority for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority). If you do not use the `order` keyword, the ACLs have the lowest order by default as **255**.
fragments	Enter the keyword `fragments` to use ACLs to control packet fragments.
log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated. with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The time interval range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL

in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

ACCESS-LIST

Command History

Version 9.4(0.0)	Added the support for flow-based monitoring on theMXL 10/40GbE Switch IO Module platform.
Version 9.3(0.0)	Added the support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.

Usage Information

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress directions. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

7

Access Control List (ACL) VLAN Groups and Content Addressable Memory (CAM)

This chapter describes the access control list (ACL) VLAN group and content addressable memory (CAM) enhancements.

member vlan

Add VLAN members to an ACL VLAN group.

Syntax `member vlan {VLAN-range}`

Parameters

VLAN-range	Enter the member VLANs using comma-separated VLAN IDs, a range of VLAN IDs, a single VLAN ID, or a combination. For example: Comma-separated: 3, 4, 6 Range: 5-10 Combination: 3, 4, 5-10, 8

Default None

Command Modes CONFIGURATION (conf-acl-vl-grp)

Command History

Version 9.3(0.0)	Introduced on the MXL platform.

Usage Information

At a maximum, there can be only 32 VLAN members in all ACL VLAN groups. A VLAN can belong to only one group at any given time.

You can create an ACL VLAN group and attach the ACL with the VLAN members. The optimization is applicable only when you create an ACL VLAN group. If you apply an ACL separately on the VLAN interface, each ACL has a mapping with the VLAN and increased CAM space utilization occurs.

Attaching an ACL individually to VLAN interfaces is similar to the behavior of ACL-VLAN mapping storage in CAM prior to the implementation of the ACL VLAN group functionality.

ip access-group

Apply an egress IP ACL to the ACL VLAN group.

Syntax

```
ip access-group {group name} out implicit-permit
```

Parameters

group-name	Enter the name of the ACL VLAN group where you want the egress IP ACLs applied, up to 140 characters.
out	Enter the keyword `out` to apply the ACL to outgoing traffic.
implicit-permit	Enter the keyword `implicit-permit` to change the default action of the ACL from implicit-deny to implicit-permit (that is, if the traffic does not match the filters in the ACL, the traffic is permitted instead of dropped).

Default None

Command Modes CONFIGURATION (conf-acl-vl-grp)

Command History

Version 9.3(0.0)	Introduced on the MXL 10/40GbE Switch IO Module platform.

Usage Information You can apply only an egress IP ACL on an ACL VLAN group.

show acl-vlan-group

Display all the ACL VLAN groups or display a specific ACL VLAN group, identified by name.

Syntax

```
show acl-vlan-group {group-name | detail}
```

Parameters

group-name	(Optional) Display only the ACL VLAN group that is specified, up to 140 characters.
detail	Display information in a line-by-line format to display the names in their entirety. Without the detail option, the output displays in a table style and information may be truncated.

Default No default behavior or values

Command Modes

EXEC

EXEC Privilege

Command History	Version 9.3(0.0)	Introduced on the MXL 10/40GbE Switch IO Module platform.

Usage Information

When an ACL-VLAN-Group name or the Access List Group Name contains more than 30 characters, the name is truncated in the show `acl-vlan-group` command output.

Examples

The following sample illustrates the output of the `show acl-vlan-group` command.

NOTE: Some group names and some access list names are truncated.

```
Dell#show acl-vlan-group
Group Name                    Egress IP Acl                 Vlan
Members
TestGroupSeventeenTwenty      SpecialAccessOnlyExperts
100,200,300
CustomerNumberIdentifica      AnyEmployeeCustomerEleve      2-10,99
HostGroup                     Group5                        1,1000

Dell#
```

The following sample output is displayed when using the `show acl-vlan-group` *`group-name`* option.

NOTE: The access list name is truncated.

```
Dell#show acl-vlan-group TestGroupSeventeenTwenty
Group Name                    Egress IP Acl                 Vlan
Members
TestGroupSeventeenTwenty      SpecialAccessOnlyExperts
100,200,300

Dell#
```

The following sample output shows the line-by-line style display when using the `show acl-vlan-group detail` option.

NOTE: No group or access list names are truncated

```
Dell#show acl-vlan-group detail

Group Name :
  TestGroupSeventeenTwenty
Egress IP Acl :
  SpecialAccessOnlyExpertsAllowed
Vlan Members :
  100,200,300

Group Name :
  CustomerNumberIdentificationEleven
Egress IP Acl :
  AnyEmployeeCustomerElevenGrantedAccess
Vlan Members :
  2-10,99

Group Name :
  HostGroup
Egress IP Acl :
  Group5
Vlan Members :
  1,1000
Dell#
```

show cam-acl-vlan

Display the number of flow processor (FP) blocks that is allocated for the different VLAN services.

Syntax

`show cam-acl-vlan`

Command Modes

EXEC Privilege

Command History

Version 9.3.(0.0)	Introduced on the MXL 10/40GbE Switch IO Module platform.

Usage Information

After CAM configuration for ACL VLAN groups is performed, you must reboot the system to enable the settings to be stored in nonvolatile storage. During the initialization of CAM, the chassis manager reads the NVRAM and allocates the dynamic VCAP regions.

The following table describes the output fields of this `show` command:

Field	Description
Chassis Vlan Cam ACL	Details about the CAM blocks allocated for ACLs for various VLAN operations at a system-wide, global level.
Stack Unit <number>	Details about the CAM blocks allocated for ACLs for various VLAN operations for a particular stack unit.
Current Settings(in block sizes)	Information about the number of FP blocks that are currently in use or allocated.
VlanOpenFlow	Number of FP blocks for VLAN open flow operations.
VlanIscsi	Number of FP blocks for VLAN internet small computer system interface (iSCSI) counters.
VlanHp	Number of FP blocks for VLAN high performance processes.
VlanFcoe	Number of FP blocks for VLAN Fiber Channel over Ethernet (FCoE) operations.

Field	Description
VlanAclOpt	Number of FP blocks for ACL VLAN optimzation feature.

Example

```
Dell#show cam-acl-vlan
-- Chassis Vlan Cam ACL --
             Current Settings(in block sizes)
VlanOpenFlow :         0
VlanIscsi    :         2
VlanHp       :         1
VlanFcoe     :         1
VlanAclOpt :         0

-- Stack unit 0 --
           Current Settings(in block sizes)
VlanOpenFlow :         0
VlanIscsi    :         2
VlanHp       :         1
VlanFcoe     :         1
VlanAclOpt :          0
```

cam-acl-vlan

Allocate the number of flow processor (FP) blocks or entries for VLAN services and processes.

Syntax

`cam-acl-vlan { default | vlanopenflow <0-2> | vlaniscsi <0-2> | vlanaclopt <0-2>`

Parameters

default	Reset the number of FP blocks to default. By default, 0 groups are allocated for the ACL in VCAP. ACL VLAN groups or CAM optimization is not enabled by default, and you need to allocate the slices for CAM optimization.
vlanopenflow <0-2>	Allocate the number of FP blocks for VLAN open flow operations.
vlaniscsi <0-2>	Allocate the number of FP blocks for VLAN iSCSI counters.
vlanaclopt <0-2>	Allocate the number of FP blocks for the ACL VLAN optimization feature.

Default

If you use the `default` keyword with the `cam-acl-vlan` command, the FP blocks allocated for VLAN processes are restored to their default values. No FP blocks or dynamic VLAN Content Aware Processor (VCAP) groups are allocated for VLAN operations by default.

Command Modes

CONFIGURATION

Command History	Version 9.3(0.0)	Introduced on the MXL platform.

Usage Information

The VLAN ContentAware Processor (VCAP) application is a pre-ingress CAP that modifies the VLAN settings before packets are forwarded. To support the ACL CAM optimization functionality, the CAM carving feature is enhanced. A total of four VACP groups are present, of which two are for fixed groups and the other two are for dynamic groups. Out of the total of two dynamic groups, you can allocate zero, one, or two flow processor (FP) blocks to iSCSI Counters, OpenFlow and ACL Optimization. You can configure only two of these features at a point in time.

show cam-usage

View the amount of CAM space available, used, and remaining in each partition (including IPv4Flow and Layer 2 ACL sub-partitions).

Syntax

`show cam-usage [acl | router | switch]`

Parameters

acl	(OPTIONAL) Enter the keyword `acl` to display Layer 2 and Layer 3 ACL CAM usage.
router	(OPTIONAL) Enter the keyword `router` to display Layer 3 CAM usage.
switch	(OPTIONAL) Enter the keyword `switch` to display Layer 2 CAM usage.

Command Modes

EXEC

EXEC Privilege

Command History	Version 9.3(0.0)	Introduced on the MXL 10/40GbE Switch IO Module platform.

Usage Information

The following regions must be provided in the `show cam-usage` output:

- L3AclCam
- L2AclCam
- V6AclCam

The following table describes the output fields of this `show` command:

Field	Description
LineCard	Number of the line card that contains information on ACL VLAN groups
Portpipe	The hardware path that packets follow through a system for ACL optimization
CAM-Region	Type of area in the CAM block that is used for ACL VLAN groups
Total CAM space	Total amount of space in the CAM block
Used CAM	Amount of CAM space that is currently in use
Available CAM	Amount of CAM space that is free and remaining to be allocated for ACLs

Example 1: Output of the show cam-usage Command

```
Dell#show cam-usage
Linecard|Portpipe| CAM Partition   | Total CAM   |  Used CAM
|Available CAM
========|========|=================|=============|
=============|==============
    1   |   0    | IN-L2 ACL       |     1008    |      320
|       688
        |        | IN-L2 FIB       |    32768    |     1132
|     31636
        |        | IN-L3 ACL       |    12288    |        2
|     12286
        |        | IN-L3 FIB       |   262141    |       14
|    262127
        |        | IN-L3-SysFlow   |     2878    |       45
|      2833
        |        | IN-L3-TrcList   |     1024    |        0
|      1024
        |        | IN-L3-McastFib  |     9215    |        0
|      9215
        |        | IN-L3-Qos       |     8192    |        0
|      8192
        |        | IN-L3-PBR       |     1024    |        0
|      1024
        |        | IN-V6 ACL       |        0    |        0
|         0
        |        | IN-V6 FIB       |        0    |        0
|         0
        |        | IN-V6-SysFlow   |        0    |        0
|         0
        |        | IN-V6-McastFib  |        0    |        0
|         0
        |        | OUT-L2 ACL      |     1024    |        0
|      1024
        |        | OUT-L3 ACL      |     1024    |        0
|      1024
        |        | OUT-V6 ACL      |        0    |        0
|         0
    1   |   1    | IN-L2 ACL       |      320    |        0
|       320
        |        | IN-L2 FIB       |    32768    |     1136
|     31632
        |        | IN-L3 ACL       |    12288    |        2
|     12286
        |        | IN-L3 FIB        |    262141   |         14
|    262127
        |        | IN-L3-SysFlow    |      2878   |         44
|      2834
--More--
```

Example 2: Output of the show cam-usage acl Command

```
Dell#show cam-usage acl
Linecard|Portpipe| CAM Partition   | Total CAM   |  Used CAM
|Available CAM
========|========|=================|=============|
=============|============
   11   |   0    | IN-L2 ACL        |      1008   |
0    |      1008
        |        | IN-L3 ACL        |     12288   |
2    |     12286
        |        | OUT-L2 ACL       |      1024   |
2    |      1022
        |        | OUT-L3 ACL       |      1024   |
0    |      1024
```

Example 3: Output of the show cam-usage router Command

```
Dell#show cam-usage router
Linecard|Portpipe| CAM Partition   | Total CAM   |  Used CAM
|Available CAM
========|========|=================|=============|
=============|==============
   11   |   0    | IN-L3 ACL        |      8192   |          3
|      8189
        |        | IN-L3 FIB        |    196607   |          1
|    196606
        |        | IN-L3-SysFlow    |      2878   |          0
|      2878
        |        | IN-L3-TrcList    |      1024   |          0
|      1024
        |        | IN-L3-McastFib   |      9215   |          0
|      9215
        |        | IN-L3-Qos        |      8192   |          0
|      8192
        |        | IN-L3-PBR        |      1024   |          0
|      1024
        |        | OUT-L3 ACL       |     16384   |          0
|     16384
   11   |   1    | IN-L3 ACL        |      8192   |          3
|      8189
        |        | IN-L3 FIB        |    196607   |          1
|    196606
        |        | IN-L3-SysFlow    |      2878   |          0
|      2878
        |        | IN-L3-TrcList    |      1024   |          0
|      1024
        |        | IN-L3-McastFib   |      9215   |          0
|      9215
        |        | IN-L3-Qos        |      8192   |          0
|      8192
        |        | IN-L3-PBR        |      1024   |          0
|      1024
        |        | OUT-L3 ACL       |     16384   |          0
|     16384
```

Example 4: Output of the show cam-usage switch Command

```
Dell#show cam-usage switch

Linecard|Portpipe| CAM Partition   | Total CAM    |  Used CAM
|Available CAM
========|========|=================|=============|
=============|==============
   11   |   0    | IN-L2 ACL       |      7152   |          0
|      7152
        |        | IN-L2 FIB       |     32768   |       1081
|     31687
        |        | OUT-L2 ACL      |         0   |          0
|         0
   11   |   1    | IN-L2 ACL       |      7152   |          0
|      7152
        |        | IN-L2 FIB       |     32768   |       1081
|     31687
        |        | OUT-L2 ACL      |         0   |          0
|         0
```

show running config acl-vlan-group

Display the running configuration of all or a given ACL VLAN group.

Syntax `show running config acl-vlan-group` *`group name`*

Parameters

group-name	Display only the ACL VLAN group that is specified. The maximum group name is 140 characters.

Default None

Command Modes

EXEC

EXEC Privilege

Command History

Version 9.3(0.0)	Introduced on the MXL 10/40GbE Switch IO Module platform.

Examples The following sample output shows the line-by-line style display when using the `show running-config acl-vlan-group` option. Note that no group or access list names are truncated

```
Dell#show running-config acl-vlan-group
!
acl-vlan-group group1
 description Acl Vlan Group1
 member vlan 1-10,400-410,500
 ip access-group acl1 out implicit-permit
!
acl-vlan-group group2
 member vlan 20
 ip access-group acl2 out
Dell#
```

```
Dell#show running-config acl-vlan-group group1
!
acl-vlan-group group1
 description Acl Vlan Group1
 member vlan 1-10,400-410,500
 ip access-group acl1 out implicit-permit

Dell#
```

acl-vlan-group

Create an ACL VLAN group.

Syntax

`acl-vlan-group {`*`group name`*`}`

To remove an ACL VLAN group, use the `no acl-vlan-group {`*`group name`*`}` command.

Parameters

group-name	Specify the name of the ACL VLAN group. The name can contain a maximum 140 characters.

Default

No default behavior or values

Command Modes

CONFIGURATION

Command History

Version 9.3(0.0)	Introduced on the MXL 10/40GbE Switch IO Module platform.

Usage Information

You can have up to eight different ACL VLAN groups at any given time. When you configure an ACL VLAN group, you enter the ACL VLAN Group Configuration mode.

To avoid the problem of excessive consumption of CAM area, you can configure ACL VLAN groups that combines all the VLANs that are applied with the same ACL in a single group. A unique identifier for each of ACL attached to the VLAN is used as a handle or locator in the CAM area instead of the VLAN id. This method of processing signficiantly reduces the number of entries in the CAM area and saves memory space in CAM.

You can create an ACL VLAN group and attach the ACL with the VLAN members. Optimization is applicable only when you create an ACL VLAN group. If you apply an ACL separately on the VLAN interface, each ACL maps with the VLAN and increased CAM space utilization occurs.

Attaching an ACL individually to VLAN interfaces is similar to the behavior of ACL-VLAN mapping storage in CAM prior to the implementation of the ACL VLAN group functionality.

show acl-vlan-group detail

Display all the ACL VLAN Groups or display a specific ACL VLAN Group by name. To display the names in their entirety, the output displays in a line-by-line format.

Syntax	`show acl-vlan-group detail`	
Parameters	**detail**	Display information in a line-by-line format to display the names in their entirety. Without the detail option, the output is displayed in a table style and information may be truncated.
Default	No default behavior or values	
Command Modes	EXEC EXEC Privilege	
Command History	**Version 9.3(0.0)**	Introduced on the MXL 10/40GbE Switch IO Module platform.
Usage Information	The output for this command displays in a line-by-line format. This allows the ACL-VLAN-Group names (or the Access List Group Names) to display in their entirety.	
Examples	The following sample output shows the line-by-line style display when using the `show acl-vlan-group detail` option. Note that no group or access list names are truncated	

```
Dell#show acl-vlan-group detail

Group Name :
  TestGroupSeventeenTwenty
Egress IP Acl :
  SpecialAccessOnlyExpertsAllowed
Vlan Members :
  100,200,300

Group Name :
  CustomerNumberIdentificationEleven
Egress IP Acl :
  AnyEmployeeCustomerElevenGrantedAccess
Vlan Members :
  2-10,99

Group Name :
  HostGroup
Egress IP Acl :
  Group5
Vlan Members :
  1,1000
Dell#
```

description (ACL VLAN Group)

Add a description to the ACL VLAN group.

Syntax	`description` *`description`*
Parameters	*description* — Enter a description to identify the ACL VLAN group (80 characters maximum).
Default	No default behavior or values
Command Modes	CONFIGURATION (conf-acl-vl-grp)
Command History	Version 9.3(0.0) — Introduced on the MXL 10/40GbE Switch IO Module platform.
Usage Information	Enter a description for each ACL VLAN group that you create for effective and streamlined administrative and logging purposes.

8

Bidirectional Forwarding Detection (BFD)

Bidirectional forwarding detection (BFD) is a detection protocol that provides fast forwarding path failure detection.

The Dell Networking Operating System (OS) implementation is based on the standards specified in the IETF Draft draft-ietf-bfd-base-03 and supports BFD on all Layer 3 physical interfaces including virtual local area network (VLAN) interfaces and port-channels.

bfd all-neighbors

Enable BFD sessions with all neighbors discovered by Layer 3 protocols intermediate system to intermediate system (IS-IS), open shortest path first (OSPF), OSPFv3, or border gateway protocol (BGP) on router interfaces, and (optionally) reconfigure the default timer values.

Syntax

```
[vrrp] bfd all-neighbors [interval interval min_rx min_rx
multiplier value role {active | passive}]
```

Parameters

vrrp	Enter the keyword `vrrp` in INTERFACE mode to enable BFD for VRRP.
interval *milliseconds*	(OPTIONAL) Enter the keyword `interval` to specify non-default BFD session parameters beginning with the transmission interval. The range is from 50 to 1000. The default is **100**.
min_rx *milliseconds*	Enter the keyword `min_rx` to specify the minimum rate at which the local system would like to receive control packets from the remote system. The range is from 50 to 100. The default is **100**.
multiplier *value*	Enter the keyword `multiplier` to specify the number of packets that must be missed in order to declare a session down. The range is from 3 to 50. The default is **3**.
role [active | passive]	Enter the role that the local system assumes: • `Active` — The active system initiates the BFD session. Both systems can be active for the same session. • `Passive` — The passive system does not initiate a session. It only responds to a request for session initialization from the active system. The default is **active**.

Defaults

Refer to *Parameters*.

Command Modes

ROUTER OSPF

ROUTER OSPFv3

ROUTER BGP

ROUTER ISIS

INTERFACE (BFD for VRRP only)

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

All neighbors inherit the timer values configured with the `bfd neighbor` command except in the following cases:

- Timer values configured with the `isis bfd all-neighbors` commands in INTERFACE mode override timer values configured with the `bfd neighbor` command. Likewise, using the `no bfd neighbor` command does not disable BFD on an interface if you explicitly enable BFD using the `isis bfd all-neighbors` command.
- Neighbors that have been explicitly enabled or disabled for a BFD session with the `bfd neighbor` or `neighbor bfd disable` commands in ROUTER BGP mode do not inherit the global BFD enable/disable values configured with the `bfd neighbor` command or configured for the peer group to which a neighbor belongs. The neighbors inherit only the global timer values (configured with the `bfd neighbor` command).

Related Commands

show bfd neighbors — displays BFD neighbor information on all interfaces or a specified interface.

bfd neighbor — explicitly enables a BFD session with a BGP neighbor or a BGP peer group.

neighbor bfd disable — explicitly disables a BFD session with a BGP neighbor or a BGP peer group.

bfd disable

Disable BFD on an interface.

Syntax

`bfd disable`

Re-enable BFD using the `no bfd disable` command.

Defaults

BFD is disabled by default.

Command Modes	INTERFACE VRRP
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.

bfd enable (Configuration)

Enable BFD on all interfaces.

Syntax	`bfd enable` Disable BFD using the `no bfd enable` command.
Defaults	BFD is disabled by default.
Command Modes	CONFIGURATION
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.

bfd enable (Interface)

Enable BFD on an interface.

Syntax	`bfd enable`
Defaults	BFD is enabled on all interfaces when you enable BFD from CONFIGURATION mode.
Command Modes	INTERFACE
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.

bfd interval

Specify non-default BFD session parameters beginning with the transmission interval.

Syntax

```
bfd interval interval min_rx min_rx multiplier value role
{active | passive}
```

Parameters

interval *milliseconds*	Enter the keywords `interval` to specify non-default BFD session parameters beginning with the transmission interval. The range is from 50 to 1000. The default is **100**.
min_rx *milliseconds*	Enter the keywords `min_rx` to specify the minimum rate at which the local system would like to receive control packets from the remote system. The range is from 50 to 1000. The default is **100**.
multiplier *value*	Enter the keywords `multiplier` to specify the number of packets that must be missed in order to declare a session down. The range is from 3 to 50. The default is **3**.
role [active | passive]	Enter the role that the local system assumes: • `Active` — The active system initiates the BFD session. Both systems can be active for the same session. • `Passive` — The passive system does not initiate a session. It only responds to a request for session initialization from the active system. The default is **Active**.

Defaults: Refer to *Parameters*.

Command Modes: INTERFACE

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell(conf-if-gi-0/3)#bfd interval 250 min_rx 300 multiplier 4
role passive
Dell(conf-if-gi-0/3)#
```

bfd neighbor

Establish a BFD session with a neighbor.

Syntax: `bfd neighbor` *`ip-address`*

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format (A.B.C.D).

Defaults: none

Command Modes: INTERFACE

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

show bfd neighbors — displays the BFD neighbor information on all interfaces or a specified interface.

bfd protocol-liveness

Enable the BFD protocol liveness feature.

Syntax

```
bfd protocol-liveness
```

Defaults

Disabled

Command Modes

CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Protocol Liveness is a feature that notifies the BFD Manager when a client protocol (for example, OSPF and ISIS) is disabled. When a client is disabled, all BFD sessions for that protocol are torn down. Neighbors on the remote system receive an Admin Down control packet and are placed in the Down state. Peer routers might take corrective action by choosing alternative paths for the routes that originally pointed to this router.

ip route bfd

Enable BFD for all neighbors configured through static routes.

Syntax

```
ip route bfd [interval interval min_rx min_rx multiplier value
role {active | passive}]
```

To disable BFD for all neighbors configured through static routes, use the `no ip route bfd [interval interval min_rx min_rx multiplier value role {active | passive}]` command.

Parameters

interval *milliseconds*	(OPTIONAL) Enter the keywords `interval` to specify non-default BFD session parameters beginning with the transmission interval. The range is from 50 to 1000. The default is **100**.
min_rx *milliseconds*	Enter the keywords `min_rx` to specify the minimum rate at which the local system receives control packets from the remote system. The range is from 50 to 1000. The default is **100**.

multiplier *value*	Enter the keywords `multiplier` to specify the number of packets that must be missed in order to declare a session down. The range is from 3 to 50. The default is **3**.
role [active | passive]	Enter the role that the local system assumes: • `Active` — The active system initiates the BFD session. Both systems can be active for the same session. • `Passive` — The passive system does not initiate a session. It only responds to a request for session initialization from the active system. The default is **Active**.

Defaults

See Parameters

Command Modes

CONFIGURATION

Command History

Version 9.2.(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

show bfd neighbors — displays the BFD neighbor information on all interfaces or a specified interface.

ipv6 ospf bfd all-neighbors

Establish BFD sessions with all OSPFv3 neighbors on a single interface or use non-default BFD session parameters.

Syntax

```
ipv6 ospf bfd all-neighbors [disable | [interval interval
min_rx min_rx multiplier value role {active | passive}]]
```

To disable all BFD sessions on an OSPFv3 interface implicitly, use the `no ipv6 ospf bfd all-neighbors [disable | [interval interval min_rx min_rx multiplier value role {active | passive}]]`command in interface mode..

Parameters

disable	(OPTIONAL) Enter the keyword `disable` to disable BFD on this interface.
interval *milliseconds*	(OPTIONAL) Enter the keyword `interval` to specify non-default BFD session parameters beginning with the transmission interval. The range is from 50 to 1000. The default is **100**.
min_rx *milliseconds*	Enter the keywords `min_rx` to specify the minimum rate at which the local system receives control packets from the remote system. The range is from 50 to 100. The default is **100**.

multiplier *value*	Enter the keyword `multiplier` to specify the number of packets that must be missed in order to declare a session down. The range is from 3 to 50. The default is **3**.
role [active | passive]	Enter the role that the local system assumes: • `Active` — The active system initiates the BFD session. Both systems can be active for the same session. • `Passive` — The passive system does not initiate a session. It only responds to a request for session initialization from the active system. The default is **Active**.

Defaults See Parameters

Command Modes INTERFACE

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

isis bfd all-neighbors

Enable BFD on all IS-IS neighbors discovered on an interface.

Syntax

```
isis bfd all-neighbors [disable | [interval interval min_rx
min_rx multiplier value role {active | passive}]]
```

To remove all BFD sessions with IS-IS neighbors discovered on this interface, use the `no isis bfd all-neighbors [disable | [interval interval min_rx min_rx multiplier value role {active | passive}]]` command.

Parameters

disable	(OPTIONAL) Enter the keyword `disable` to disable BFD on this interface.
interval *milliseconds*	(OPTIONAL) Enter the keywords `interval` to specify non-default BFD session parameters beginning with the transmission interval. The range is from 50 to 1000. The default is **100**.
min_rx *milliseconds*	Enter the keywords `min_rx` to specify the minimum rate at which the local system would like to receive control packets from the remote system. The range is from 50 to 1000. The default is **100**.
multiplier *value*	Enter the keywords `multiplier` to specify the number of packets that must be missed in order to declare a session down. The range is from 3 to 50. The default is **3**.

role [active | passive]	Enter the role that the local system assumes: • `Active` — The active system initiates the BFD session. Both systems can be active for the same session. • `Passive` — The passive system does not initiate a session. It only responds to a request for session initialization from the active system. The default is **Active**.

Defaults

See Parameters

Command Modes

INTERFACE

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

This command provides the flexibility to fine-tune the timer values based on individual interface needs when ISIS BFD is configured in CONFIGURATION mode. Any timer values specified with this command overrides timers set using the `bfd all-neighbors` command. Using the `no` form of this command does not disable BFD if BFD is configured in CONFIGURATION mode.

To disable BFD on a specific interface while BFD is configured in CONFIGURATION mode, use the keyword `disable`.

neighbor bfd

Explicitly enable a BFD session with a BGP neighbor or a BGP peer group.

Syntax

`neighbor {ip-address | peer-group-name} bfd`

Parameters

ip-address	Enter the IP address of the BGP neighbor that you want to explicitly enable for BFD sessions in dotted decimal format (A.B.C.D).
peer-group-name	Enter the name of the peer group that you want to explicitly enable for BFD sessions.

Defaults

none

Command Modes

ROUTER BGP

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information	When you enable a BFD session with a specified BGP neighbor or peer group using the `bfd neighbor` command, the default BFD session parameters are used (interval: **100** milliseconds, min_rx: **100** milliseconds, multiplier: **3** packets, and role: **active**) if you have not specified parameters with the `bfd neighbor` command. When you explicitly enable a BGP neighbor for a BFD session with the `bfd neighbor` command: • The neighbor does not inherit the global BFD enable values configured with the `bfd neighbor` command or configured for the peer group to which the neighbor belongs. • The neighbor only inherits the global timer values configured with the `bfd neighbor` command: interval, min_rx, and multiplier.
Related Commands	bfd neighbor — enables BFD sessions with all neighbors the Layer 3 protocols discover. neighbor bfd disable — explicitly disables a BFD session with a BGP neighbor or a BGP peer group. show bfd neighbors — displays the BFD neighbor information on all interfaces or a specified interface.

neighbor bfd disable

Explicitly disable a BFD session with a BGP neighbor or a BGP peer group.

Syntax

```
neighbor {ip-address | peer-group-name} bfd disable
```

Parameters

ip-address	Enter the IP address of the BGP neighbor that you want to explicitly disable for BFD sessions in dotted decimal format (A.B.C.D).
peer-group-name	Enter the name of the peer group that you want to explicitly disable for BFD sessions.

Defaults	none
Command Modes	ROUTER BGP
Command History	Version 9.2(0.0) — Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	When you explicitly disable a BGP neighbor for a BFD session with the `neighbor bfd disable` command:

- The neighbor does not inherit the global BFD disable values configured with the `bfd all-neighbor` command or configured for the peer group to which the neighbor belongs.
- The neighbor only inherits the global timer values configured with the `bfd all-neighbor` command: interval, min_rx, and multiplier.

When you remove the Disabled state of a BFD for a BGP session with a specified neighbor by entering the `no neighbor bfd disable` command, the BGP link with the neighbor returns to normal operation and uses the BFD session parameters globally configured with the `bfd all-neighbor` command or configured for the peer group to which the neighbor belongs.

Related Commands	bfd all-neighbors — enables BFD sessions with all neighbors discovered by Layer 3 protocols. bfd neighbor — explicitly enables a BFD session with a BGP neighbor or a BGP peer group. show bfd neighbors — displays the BFD neighbor information on all interfaces or a specified interface.

show bfd neighbors

Display BFD neighbor information on all interfaces or a specified interface.

Syntax `show bfd neighbors *interface* [detail]`

Parameters

interface	Enter one of the following keywords and slot/port or number information: • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` then the slot/port information. • For a port-channel interface, enter the keyword `port-channel` then a number. The range is from 1 to 128. • For VLAN interfaces, enter the keyword `vlan` then a number from 1 to 4094. For ExaScale VLAN interfaces, the range is 1 to 2730 (VLAN IDs can be from 0 to 4093).
detail	(OPTIONAL) Enter the keyword `detail` to view detailed information about BFD neighbors.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show bfd neighbors

*     - Active session role
Ad Dn - Admin Down
B     - BGP
C     - CLI
I     - ISIS
O     - OSPF
R     - Static Route (RTM)

  LocalAddr   RemoteAddr   Interface State Rx-int Tx-int Mult
Clients
* 10.1.3.2    10.1.3.1     Gi 1/3    Up    300    250    3    C
```

Example (Detail)

```
Dell#show bfd neighbors detail

Session Discriminator: 1
Neighbor Discriminator: 1
Local Addr: 10.1.3.2
Local MAC Addr: 00:01:e8:02:15:0e
Remote Addr: 10.1.3.1
Remote MAC Addr: 00:01:e8:27:2b:f1
Int: GigabitEthernet 1/3
State: Up
Configured parameters:
 TX: 100ms, RX: 100ms, Multiplier: 3
Neighbor parameters:
 TX: 250ms, RX: 300ms, Multiplier: 4
Actual parameters:
 TX: 300ms, RX: 250ms, Multiplier: 3
Role: Active
Delete session on Down: False
Client Registered: CLI
Uptime: 00:02:04
Statistics:
 Number of packets received from neighbor: 376
 Number of packets sent to neighbor: 314
 Number of state changes: 2
 Number of messages from IFA about port state change: 0
 Number of messages communicated b/w Manager and Agent: 6
Dell#
```

Related Commands

bfd neighbor — establishes a BFD session with a neighbor.

bfd all-neighbors — establishes BFD sessions with all neighbors discovered by the IS-IS protocol or OSPF protocol out of all interfaces.

vrrp bfd neighbor

Establish a BFD for VRRP session with a neighbor.

Syntax	`vrrp bfd neighbor` *`ip-address`*
Parameters	**neighbor** ***ip-address***: Enter the IP address of the BFD neighbor.
Defaults	none
Command Modes	INTERFACE
Command History	**Version 9.2(0.0)**: Introduced on the MXL 10/40GbE Switch IO Module.

9

Border Gateway Protocol IPv4 (BGPv4)

For detailed information about configuring BGP, refer to the BGP chapter in the *Dell Networking OS Configuration Guide*.

This chapter contains the following sections:

- BGPv4 Commands
- MBGP Commands
- BGP Extended Communities (RFC 4360)

BGP IPv6 Commands are listed in the following sections:

- IPv6 BGP Commands
- IPv6 MBGP Commands

BGPv4 Commands

Border gateway protocol (BGP) is an external gateway protocol that transmits interdomain routing information within and between autonomous systems (AS).

BGP version 4 (BGPv4) supports classless interdomain routing (CIDR) and the aggregation of routes and AS paths. Basically, two routers (called neighbors or peers) exchange information including full routing tables and periodically send messages to update those routing tables.

NOTE: Dell Networking OS Version 7.7.1 supports 2-Byte (16-bit) and 4-Byte (32-bit) format for autonomous system numbers (ASNs), where the 2-Byte format is 1-65535 and the 4-Byte format is 1-4294967295.

NOTE: Dell Networking OS Version 8.3.1.0 supports dotted format as well as the traditional plain format for AS numbers. Display the dot format using the `show ip bgp` commands. To determine the comparable dot format for an ASN from a traditional format, use `ASN/65536. ASN%65536`. For more information about using the 2–Byte or 4-Byte format, refer to the *Dell Networking OS Configuration Guide*.

address-family

Enable the IPv4 multicast or the IPv6 address family.

Syntax `address-family [ipv4 multicast| ipv6unicast]`

Parameters

ipv4 multicast	Enter BGPv4 multicast mode.

ipv6 unicast	Enter BGPv6 mode.

Defaults Not configured.

Command Modes ROUTER BGP

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

aggregate-address

To minimize the number of entries in the routing table, summarize a range of prefixes.

Syntax

```
aggregate-address ip-address mask [advertise-map map-name] [as-set] [attribute-map map-name] [summary-only] [suppress-map map-name]
```

Parameters

ip-address mask	Enter the IP address and mask of the route to be the aggregate address. Enter the IP address in dotted decimal format (A.B.C.D) and mask in /prefix format (/x).
advertise-map *map-name*	(OPTIONAL) Enter the keywords `advertise-map` then the name of a configured route map to set filters for advertising an aggregate route.
as-set	(OPTIONAL) Enter the keyword `as-set` to generate path attribute information and include it in the aggregate. AS_SET includes AS_PATH and community information from the routes included in the aggregated route.
attribute-map *map-name*	(OPTIONAL) Enter the keywords `attribute-map` then the name of a configured route map to modify attributes of the aggregate, excluding AS_PATH and NEXT_HOP attributes.
summary-only	(OPTIONAL) Enter the keyword `summary-only` to advertise only the aggregate address. Specific routes are not advertised.
suppress-map *map-name*	(OPTIONAL) Enter the keywords `suppress-map` then the name of a configured route map to identify which more-specific routes in the aggregate are suppressed.

Defaults Not configured.

Command Modes

- ROUTER BGP ADDRESS FAMILY
- ROUTER BGP ADDRESS FAMILY IPv6

Command History	**Version 9.2(0.0)**	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

At least one of the routes included in the aggregate address must be in the BGP routing table for the configured aggregate to become active.

If routes within the aggregate are constantly changing, do not add the `as-set` parameter to the aggregate as the aggregate flaps to keep track of the changes in the AS_PATH.

In route maps used in the `suppress-map` parameter, routes meeting the `deny` clause are not suppress; in other words, they are allowed. The opposite is also true: routes meeting the `permit` clause are suppressed.

If the route is injected via the `network` command, that route still appears in the routing table if the `summary-only` parameter is configured in the `aggregate-address` command.

The `summary-only` parameter suppresses all advertisements. If you want to suppress advertisements to only specific neighbors, use the `neighbor distribute-list` command.

In the `show ip bgp` command, aggregates contain an 'a' in the first column and routes suppressed by the aggregate contain an 's' in the first column.

bgp add-path

Allow the advertisement of multiple paths for the same address prefix without the new paths replacing any previous ones.

Syntax `bgp add-path [send | receive | both] path-count`

Parameters

send	Enter the keyword `send` to indicate that the system sends multiple paths to peers.
receive	Enter the keyword `receive` to indicate that the system accepts multiple paths from peers.
both	Enter the keyword `both` to indicate that the system sends and accepts multiple paths from peers.
path-count	Enter the number paths supported. The range is from 2 to 64.

Defaults Disabled

Command Modes

- ROUTER BGP
- ROUTER BGP-address-family

Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	neighbor add-path — specifies that this neighbor/peer group can send/receive multiple path advertisements.

bgp always-compare-med

Allows you to enable comparison of the MULTI_EXIT_DISC (MED) attributes in the paths from different external ASs.

Syntax	`bgp always-compare-med` To disable comparison of MED, enter `no bgp always-compare-med`.
Defaults	Disabled (that is, the software only compares MEDs from neighbors within the same AS).
Command Modes	ROUTER BGP
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	Any update without a MED attribute is the least preferred route. If you enable this command, use the `clear ip bgp *` command to recompute the best path.

bgp asnotation

Allows you to implement a method for AS number representation in the command line interface (CLI).

Syntax	`bgp asnotation [asplain | asdot+ | asdot]` To disable a dot or dot+ representation and return to ASPLAIN, enter the `no bgp asnotation` command.
Defaults	**asplain**
Command Modes	ROUTER BGP
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Before enabling this feature, enable the `enable bgp four-octet-as-support`command. If you disable the `four-octect-support` command after using dot or dot+ format, the AS numbers revert to asplain text.

When you apply an asnotation, it is reflected in the running-configuration. If you change the notation type, the running-config updates dynamically and the new notation shows.

Example

```
Dell(conf)#router bgp 1
Dell(conf-router_bgp)#bgp asnotation asdot
Dell(conf-router_bgp)#ex
Dell(conf)#do show run | grep bgp

router bgp 1
  bgp four-octet-as-support
  bgp asnotation asdot

Dell(conf)#router bgp 1
Dell(conf-router_bgp)#bgp asnotation asdot+
Dell(conf-router_bgp)#ex

Dell(conf)#do show run | grep bgp
router bgp 1
  bgp four-octet-as-support
  bgp asnotation asdot+

Dell(conf)#router bgp 1
Dell(conf-router_bgp)#bgp asnotation asplain
Dell(conf-router_bgp)#ex
Dell(conf)#do show run |grep bgp
router bgp 1
  bgp four-octet-as-support

Dell(conf)#
```

Related Commands

bgp four-octet-as-support — enables 4-byte support for the BGP process.

bgp bestpath as-path ignore

Ignore the AS PATH in BGP best path calculations.

Syntax

`bgp bestpath as-path ignore`

To return to the default, enter the `no bgp bestpath as-path ignore` command.

Defaults

Disabled (that is, the software considers the AS_PATH when choosing a route as best).

Command Modes

ROUTER BGP

Command History	**Version 9.2(0.0)**	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

If you enable this command, use the `clear ip bgp *` command to recompute the best path.

bgp bestpath as-path multipath-relax

Include prefixes received from different AS paths during multipath calculation.

Syntax

```
bgp bestpath as-path multipath-relax
```

To return to the default BGP routing process, use the `no bgp bestpath as-path multipath-relax` command.

Defaults

Disabled

Command Modes

ROUTER BGP

Command History	**Version 9.2(0.0)**	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The `bestpath router bgp configuration mode` command changes the default bestpath selection algorithm. The `multipath-relax` option allows load-sharing across providers with different (but equal-length) autonomous system paths. Without this option, ECMP expects the AS paths to be identical for load-sharing.

bgp bestpath med confed

Enable MULTI_EXIT_DISC (MED) attribute comparison on paths learned from BGP confederations.

Syntax

```
bgp bestpath med confed
```

To disable MED comparison on BGP confederation paths, enter the `no bgp bestpath med confed` command.

Defaults

Disabled

Command Modes

ROUTER BGP

Command History	**Version 9.2(0.0)**	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information	The software compares the MEDs only if the path contains no external autonomous system numbers. If you enable this command, use the `clear ip bgp *` command to recompute the best path.

bgp bestpath med missing-as-best

During path selection, indicate preference to paths with missing MED (MULTI_EXIT_DISC) over paths with an advertised MED attribute.

Syntax	`bgp bestpath med missing-as-best` To return to the default selection, use the `no bgp bestpath med missing-as-best` command.
Defaults	Disabled
Command Modes	ROUTER BGP
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	The MED is a 4-byte unsigned integer value and the default behavior is to assume a missing MED as 4294967295. This command causes a missing MED to be treated as 0. During path selection, paths with a lower MED are preferred over paths with a higher MED.

bgp bestpath router-id ignore

Do not compare router-id information for external paths during best path selection.

Syntax	`bgp bestpath router-id ignore` To return to the default selection, use the `no bgp bestpath router-id ignore` command.
Defaults	Disabled
Command Modes	ROUTER BGP
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	Configuring this option retains the current best-path. When sessions are then reset, the oldest received path is chosen as the best-path.

bgp client-to-client reflection

Allows you to enable route reflection between clients in a cluster.

Syntax	`bgp client-to-client reflection` To disable client-to-client reflection, use the `no bgp client-to-client reflection` command.
Defaults	Enabled when a route reflector is configured.
Command Modes	ROUTER BGP
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	Route reflection to clients is not necessary if all client routers are fully meshed.
Related Commands	bgp cluster-id — assigns an ID to a BGP cluster with two or more route reflectors. neighbor route-reflector-client — configures a route reflector and clients.

bgp cluster-id

Assign a cluster ID to a BGP cluster with more than one route reflector.

Syntax	`bgp cluster-id {`*`ip-address`*`	`*`number`*`}` To delete a cluster ID, use the `no bgp cluster-id {`*`ip-address`*`	`*`number`*`}` command.
Parameters	*ip-address*: Enter an IP address as the route reflector cluster ID. *number*: Enter a route reflector cluster ID as a number from 1 to 4294967295.
Defaults	Not configured.
Command Modes	ROUTER BGP
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	When a BGP cluster contains only one route reflector, the cluster ID is the route reflector's router ID. For redundancy, a BGP cluster may contain two or more route reflectors. Assign a cluster ID with the `bgp cluster-id` command. Without a cluster ID, the route reflector cannot recognize route updates from the other route reflectors within the cluster.

The default format for displaying the cluster-id is dotted decimal, but if you enter the cluster-id as an integer, it is displayed as an integer.

Related Commands	bgp client-to-client reflection — enables route reflection between the route reflector and clients. neighbor route-reflector-client — configures a route reflector and clients. show ip bgp cluster-list — views paths with a cluster ID.

bgp confederation identifier

Configure an identifier for a BGP confederation.

Syntax

```
bgp confederation identifier as-number
```

To delete a BGP confederation identifier, use the `no bgp confederation identifier as-number` command.

Parameters

as-number	Enter the AS number. The range is from 0 to 65535 (2 byte), from 1 to 4294967295 (4 byte), or from 0.1 to 65535.65535 (dotted format).

Defaults: Not configured.

Command Modes: ROUTER BGP

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To accept 4-byte formats before entering a 4-byte AS number, configure your system. All the routers in the Confederation must be 4 byte or 2 byte identified routers. You cannot mix them.

The autonomous systems configured in this command are visible to the EBGP neighbors. Each autonomous system is fully meshed and contains a few connections to other autonomous systems. The next hop, MED, and local preference information is preserved throughout the confederation.

The system accepts confederation EBGP peers without a LOCAL_PREF attribute. The software sends AS_CONFED_SET and accepts AS_CONFED_SET and AS_CONF_SEQ.

Related Commands: bgp four-octet-as-support — enables 4-byte support for the BGP process.

bgp confederation peers

Specify the autonomous systems (ASs) that belong to the BGP confederation.

Syntax	`bgp confederation peers` *`as-number`* `[...`*`as-number`*`]` To return to the default, use the `no bgp confederation peers` command.
Parameters	

as-number	Enter the AS number. The range is from 0 to 65535 (2 byte), from 1 to 4294967295 (4 byte), or from 0.1 to 65535.65535 (dotted format).
...as-number	(OPTIONAL) Enter up to 16 confederation numbers. The range is from 0 to 65535 (2 byte), from 1 to 4294967295 (4 byte), or from 0.1 to 65535.65535 (dotted format).

Defaults	Not configured.
Command Modes	ROUTER BGP
Command History	

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

All the routers in the Confederation must be 4 byte or 2 byte identified routers. You cannot mix them.

The autonomous systems configured in this command are visible to the EBGP neighbors. Each autonomous system is fully meshed and contains a few connections to other autonomous systems.

After specifying autonomous systems numbers for the BGP confederation, recycle the peers to update their configuration.

Related Commands

bgp confederation identifier — configures a confederation ID.

bgp four-octet-as-support — enables 4-byte support for the BGP process.

bgp dampening

Enable BGP route dampening and configure the dampening parameters.

Syntax

`bgp dampening [`*`half-life reuse suppress max-suppress-time`*`] [route-map` *`map-name`*`]`

To disable route dampening, use the `no bgp dampening [`*`half-life reuse suppress max-suppress-time`*`] [route-map` *`map-name`*`]` command.

Parameters

half-life	(OPTIONAL) Enter the number of minutes after which the Penalty is decreased. After the router assigns a Penalty of 1024 to a route, the Penalty is decreased by half after the half-life period expires. The range is from 1 to 45. The default is **15 minutes**.
reuse	(OPTIONAL) Enter a number as the reuse value, which is compared to the flapping route’s Penalty value. If the Penalty value is less than the reuse value, the flapping route is once again advertised (or no longer suppressed). The range is from 1 to 20000. The default is **750**.
suppress	(OPTIONAL) Enter a number as the suppress value, which is compared to the flapping route’s Penalty value. If the Penalty value is greater than the suppress value, the flapping route is no longer advertised (that is, it is suppressed). The range is from 1 to 20000. The default is **2000**.
max-suppress-time	(OPTIONAL) Enter the maximum number of minutes a route can be suppressed. The default is four times the half-life value. The range is from 1 to 255. The default is **60 minutes**.
route-map *map-name*	(OPTIONAL) Enter the keyword `route-map` then the name of a configured route map. Only `match` commands in the configured route map are supported.

Defaults

Disabled.

Command Modes

- ROUTER BGP
- ROUTER BGP-address-family

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

If you enter the `bgp dampening` command, the default values for *`half-life`*, *`reuse`*, *`suppress`*, and *`max-suppress-time`* are applied. The parameters are position-dependent; therefore, if you configure one parameter, configure the parameters in the order they appear in the CLI.

Related Commands

show ip bgp dampened-paths — views the BGP paths.

bgp default local-preference

Change the default local preference value for routes exchanged between internal BGP peers.

Syntax

`bgp default local-preference value`

To return to the default value, use the `no bgp default local-preference` command.

Parameters

value	Enter a number to assign to routes as the degree of preference for those routes. When routes are compared, the higher the degree of preference or local preference value, the more the route is preferred. The range is from 0 to 4294967295. The default is **100**.

Defaults

100

Command Modes

ROUTER BGP

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

All routers apply the `bgp default local-preference` command setting within the AS. To set the local preference for a specific route, use the `set local-preference` command in ROUTE-MAP mode.

Related Commands

set metric — assigns a local preference value for a specific route.

bgp enforce-first-as

Disable (or enable) enforce-first-as check for updates received from EBGP peers.

Syntax

`bgp enforce-first-as`

To turn off the default, use the `no bgp enforce-first-as` command.

Defaults

Enabled

Command Modes

ROUTER BGP

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

This command is enabled by default, that is for all updates received from EBGP peers, BGP ensures that the first AS of the first AS segment is always the AS of the peer. If not, the update is dropped and a counter is increments. To view the "failed enforce-first-as check" counter, use the `show ip bgp neighbors` command.

If you disable the `enforce-first-as` command, it can be viewed using the `show ip protocols` command.

Related Commands	show ip bgp neighbors — views the information the BGP neighbors exchange. show ip protocols — views information on routing protocols.

bgp fast-external-failover

Enable the fast external failover feature, which immediately resets the BGP session if a link to a directly connected external peer fails.

Syntax	`bgp fast-external-failover` To disable fast external failover, use the `no bgp fast-external-failover` command.
Defaults	Enabled
Command Modes	ROUTER BGP
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	The `bgp fast-external-failover` command appears in the `show config` command output.

bgp four-octet-as-support

Enable 4-byte support for the BGP process.

Syntax	`bgp four-octet-as-support` To disable fast external failover, use the `no bgp four-octet-as-support` command.
Defaults	Disabled (supports 2–byte format)
Command Modes	ROUTER BGP
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information	Routers supporting 4-byte ASNs advertise that function in the OPEN message. The behavior of a 4-byte router is slightly different depending on whether it is speaking to a 2-byte router or a 4-byte router. When creating Confederations, all the routers in the Confederation must be 4 byte or 2 byte identified routers. You cannot mix them. Where the 2-byte format is from 1 to 65535, the 4-byte format is from 1 to 4294967295. Both formats are accepted and the advertisements reflect the entered format. For more information about using the 2 byte or 4-byte format, refer to the *Dell Networking OS Configuration Guide*.

bgp graceful-restart

To support graceful restart as a receiver only, enable graceful restart on a BGP neighbor, a BGP node, or designate a local router.

Syntax

```
bgp graceful-restart [restart-time seconds] [stale-path-time
seconds] [role receiver-only]
```

To return to the default, use the `no bgp graceful-restart` command.

Parameters

restart-time *seconds*	Enter the keyword `restart-time` then the maximum number of seconds to restart and bring-up all the peers. The range is from 1 to 3600 seconds. The default is **120 seconds**.
stale-path-time *seconds*	Enter the keyword `stale-path-time` then the maximum number of seconds to wait before restarting a peer’s stale paths. The default is **360 seconds**.
role receiver-only	Enter the keyword `role receiver-only` to designate the local router to support graceful restart as a receiver only.

Defaults as above

Command Modes ROUTER BGP

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

This feature is advertised to BGP neighbors through a capability advertisement. In Receiver Only mode, BGP saves the advertised routes of peers that support this capability when they restart.

BGP graceful restart is active only when the neighbor becomes established. Otherwise it is disabled. Graceful-restart applies to all neighbors with established adjacency.

bgp non-deterministic-med

Compare MEDs of paths from different autonomous systems.

Syntax

```
bgp non-deterministic-med
```

To return to the default, use the `no bgp non-deterministic-med` command.

Defaults

Disabled (that is, paths/routes for the same destination but from different ASs do not have their MEDs compared).

Command Modes

ROUTER BGP

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

In Non-Deterministic mode, paths are compared in the order in which they arrive. This method can lead to the system choosing different best paths from a set of paths, depending on the order in which they are received from the neighbors because MED may or may not get compared between adjacent paths. In Deterministic mode (`no bgp non-deterministic-med`), the system compares MED between adjacent paths within an AS group because all paths in the AS group are from the same AS.

When you change the path selection from Deterministic to Non-Deterministic, the path selection for the existing paths remains Deterministic until you enter the `clear ip bgp` command to clear existing paths.

bgp recursive-bgp-next-hop

Enable next-hop resolution through other routes learned by BGP.

Syntax

```
bgp recursive-bgp-next-hop
```

To disable next-hop resolution, use the `no bgp recursive-bgp-next-hop` command.

Defaults

Enabled

Command Modes

ROUTER BGP

Command History	**Version 9.2(0.0)**	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

This command is a *knob* to disable BGP next-hop resolution using BGP learned routes. During the next-hop resolution, only the first route that the next-hop resolves through is verified for the route's protocol source and is checked if the route is learned from BGP or not.

The `clear ip bgp` command is required for this command to take effect and to keep the BGP database consistent. Execute the `clear ip bgp` command right after executing this command.

Related Commands

clear ip bgp — clears the ip bgp.

bgp regex-eval-optz-disable

Disables the Regex Performance engine that optimizes complex regular expression with BGP.

Syntax

`bgp regex-eval-optz-disable`

To re-enable optimization engine, use the `no bgp regex-eval-optz-disable` command.

Defaults

Enabled

Command Modes

ROUTER BGP (conf-router_bgp)

Command History	**Version 9.2(0.0)**	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

BGP uses regular expressions (regex) to filter route information. In particular, the use of regular expressions to filter routes based on AS-PATHs and communities is common. In a large-scale configuration, filtering millions of routes based on regular expressions can be quite CPU intensive, as a regular expression evaluation involves generation and evaluation of complex finite state machines.

BGP policies, containing regular expressions to match as-path and communities, tend to use much CPU processing time, which in turn affects the BGP routing convergence. Additionally, the `show bgp` commands, which are filtered through regular expressions, use up CPU cycles particularly with large databases. The Regex Engine Performance Enhancement feature optimizes the CPU usage by caching and reusing regular expression evaluation results. This caching and reuse may be at the expensive of RP1 processor memory.

Examples

```
Dell(conf-router_bgp)#no bgp regex-eval-optz-disable
Dell(conf-router_bgp)#do show ip protocols
Routing Protocol is "ospf 22222"
  Router ID is 2.2.2.2
  Area               Routing for Networks
  51                 10.10.10.0/00

Routing Protocol is "bgp 1"
  Cluster Id is set to 10.10.10.0
  Router Id is set to 10.10.10.0
  Fast-external-fallover enabled
Regular expression evaluation optimization enabled
  Capable of ROUTE_REFRESH
  For Address Family IPv4 Unicast
    BGP table version is 0, main routing table version 0
    Distance: external 20 internal 200 local 200

Dell(conf-router_bgp)#
```

Related Commands

show ip protocols — views information on all routing protocols enabled and active.

bgp router-id

Assign a user-given ID to a BGP router.

Syntax

`bgp router-id` *`ip-address`*

To delete a user-assigned IP address, use the `no bgp router-id` command.

Parameters

ip-address	Enter an IP address in dotted decimal format to reset only that BGP neighbor.

Defaults

The router ID is the highest IP address of the Loopback interface or, if no Loopback interfaces are configured, the highest IP address of a physical interface on the router.

Command Modes

ROUTER BGP

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Peering sessions are reset when you change the router ID of a BGP router.

bgp soft-reconfig-backup

To avoid the peer from resending messages, use this command *only* when route-refresh is *not* negotiated.

Syntax

`bgp soft-reconfig-backup`

	To return to the default setting, use the `no bgp soft-reconfig-backup` command.
Defaults	**Off**
Command Modes	ROUTER BGP
Command History	Version 9.2(0.0) — Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	When you enable soft-reconfiguration for a neighbor and you execute the `clear ip bgp soft in` command, the update database stored in the router is replayed and updates are re-evaluated. With this command, the replay and update process is triggered only if route-refresh request is not negotiated with the peer. If the request is indeed negotiated (after executing the `clear ip bgp soft in` command), BGP sends a route-refresh request to the neighbor and receives all of the peer's updates.
Related Commands	clear ip bgp — activates inbound policies without resetting the BGP TCP session.

capture bgp-pdu neighbor

Enable capture of an IPv4 BGP neighbor packet.

Syntax	`capture bgp-pdu neighbor` *`ipv4-address`* `direction {both | rx | tx}` To disable capture of the IPv4 BGP neighbor packet, use the `no capture bgp-pdu neighbor ipv4-address` command.
Parameters	*ipv4-address*: Enter the IPv4 address of the target BGP neighbor. direction {both | rx | tx}: Enter the keyword `direction` and a direction — either `rx` for inbound, `tx` for outbound, or both.
Defaults	Not configured.
Command Modes	EXEC Privilege
Command History	Version 9.2(0.0) — Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	capture bgp-pdu max-buffer-size — specifies a size for the capture buffer. show capture bgp-pdu neighbor — displays BGP packet capture information.

capture bgp-pdu max-buffer-size

Set the size of the BGP packet capture buffer. This buffer size pertains to both IPv4 and IPv6 addresses.

Syntax

```
capture bgp-pdu max-buffer-size 100-102400000
```

Parameters

100-102400000	Enter a size for the capture buffer.

Defaults

40960000 bytes.

Command Modes

EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

capture bgp-pdu neighbor — enables capture of an IPv4 BGP neighbor packet.

show capture bgp-pdu neighbor — displays BGP packet capture information for an IPv6 address.

clear ip bgp

Reset BGP sessions. The soft parameter (BGP Soft Reconfiguration) clears the policies without resetting the TCP connection.

Syntax

```
clear ip bgp * | as-number | ip-address [flap-statistics | soft
[in | out]]
```

Parameters

*	Enter an asterisk (*) to reset all BGP sessions.
as-number	Enter the AS number to reset all neighbors belonging to that AS. The range is from 0 to 65535 (2 byte), from 1 to 4294967295 (4 byte), or from 0.1 to 65535.65535 (dotted format).
ip-address	Enter an IP address in dotted decimal format to reset all prefixes from that neighbor.
flap-statistics	(OPTIONAL) Enter the keyword `flap-statistics` to reset the flap statistics on all prefixes from that neighbor.
soft	(OPTIONAL) Enter the keyword `soft` to configure and activate policies without resetting the BGP TCP session, that is, BGP Soft Reconfiguration. NOTE: If you enter the `clear ip bgp ip-address soft` command, both inbound and outbound policies are reset.

in	(OPTIONAL) Enter the keyword `in` to activate only inbound policies.
out	(OPTIONAL) Enter the keyword `out` to activate only outbound policies.

Command Modes EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

bgp recursive-bgp-next-hop — disables next-hop resolution through other routes learned by the BGP.

bgp soft-reconfig-backup — turns on BGP Soft Reconfiguration.

clear ip bgp dampening

Clear information on route dampening and return the suppressed route to the Active state.

Syntax `clear ip bgp dampening [ip-address mask]`

Parameters

ip-address mask	(OPTIONAL) Enter an IP address in dotted decimal format and the prefix mask in slash format (/x) to clear dampening information only that BGP neighbor.

Command Modes EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information After you enter this command, the software deletes the history routes and returns the suppressed routes to the Active state.

clear ip bgp flap-statistics

Clear BGP flap statistics, which includes number of flaps and the time of the last flap.

Syntax `clear ip bgp flap-statistics [ip-address mask | filter-list as-path-name | regexp regular-expression]`

Parameters

ip-address mask	(OPTIONAL) Enter an IP address in dotted decimal format and the prefix mask in slash format (/x) to reset only that prefix.

filter-list *as-path-name*	(OPTIONAL) Enter the keywords `filter-list` then the name of a configured AS-PATH list.
regexp *regular-expression*	(OPTIONAL) Enter the keyword `regexp` then regular expressions. Use one or a combination of the following: • `.` = (period) any single character (including a white space). • `*` = (asterisk) the sequences in a pattern (0 or more sequences). • `+` = (plus) the sequences in a pattern (1 or more sequences). • `?` = (question mark) sequences in a pattern (either 0 or 1 sequences). NOTE: Enter an escape sequence (CTRL+v) prior to entering the `?` regular expression. • `[ ]` = (brackets) a range of single-character patterns. • `( )` = (parenthesis) groups a series of pattern elements to a single element. • `{ }` = (braces) minimum and the maximum match count. • `^` = (caret) the beginning of the input string. If you use the caret at the beginning of a sequence or range, it matches on everything BUT the characters specified. • `$` = (dollar sign) the end of the output string.

Command Modes

EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

If you enter the `clear ip bgp flap-statistics` command without any parameters, all statistics are cleared.

Related Commands

show debugging — views the enabled debugging operations.

show ip bgp flap-statistics — views the BGP flap statistics.

undebug all — disables all debugging operations.

clear ip bgp peer-group

Reset a peer-group’s BGP sessions.

Syntax

`clear ip bgp peer-group` *`peer-group-name`*

Parameters	*peer-group-name*	Enter the peer group name to reset the BGP sessions within that peer group.
Command Modes	EXEC Privilege	
Command History	Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

debug ip bgp

Display all information on BGP, including BGP events, keepalives, notifications, and updates.

Syntax

```
debug ip bgp [ip-address | peer-group peer-group-name] [in |
out]
```

To disable all BGP debugging, use the `no debug ip bgp` command.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group *peer-group-name*	Enter the keywords `peer-group` then the name of the peer group to debug.
in	(OPTIONAL) Enter the keyword `in` to view only information on inbound BGP routes.
out	(OPTIONAL) Enter the keyword `out` to view only information on outbound BGP routes.

Command Modes	EXEC Privilege	
Command History	Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To view information on both incoming and outgoing routes, do not include the `in` and `out` parameters in the debugging command. The `in` and `out` parameters cancel each other; for example, if you enter the `debug ip bgp in` command and then enter the `debug ip bgp out` command, you do not see information on the incoming routes.

Entering a `no debug ip bgp` command removes all configured debug commands for BGP.

Related Commands

debug ip bgp events — views information about BGP events.

debug ip bgp keepalives — views information about BGP keepalives.

debug ip bgp notifications — views information about BGP notifications.

debug ip bgp updates — views information about BGP updates.

show debugging — views enabled debugging operations.

debug ip bgp dampening

View information on routes being dampened.

Syntax	`debug ip bgp dampening [in	out]` To disable debugging, use the `no debug ip bgp dampening` command.
Parameters	**in** — (OPTIONAL) Enter the keyword `in` to view only inbound dampened routes. **out** — (OPTIONAL) Enter the keyword `out` to view only outbound dampened routes.
Command Modes	EXEC Privilege
Command History	Version 9.2(0.0) — Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	show debugging — view enabled debugging operations. show ip bgp dampened-paths — view BGP dampened routes.

debug ip bgp events

Display information on local BGP state changes and other BGP events.

Syntax

`debug ip bgp [ip-address | peer-group peer-group-name] events [in | out]`

To disable debugging, use the `no debug ip bgp [ip-address | peer-group peer-group-name] events` command.

Parameters

ip-address	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.

peer-group *peer-group-name*	(OPTIONAL) Enter the keyword `peer-group` then the name of the peer group.
in	(OPTIONAL) Enter the keyword `in` to view only events on inbound BGP messages.
out	(OPTIONAL) Enter the keyword `out` to view only events on outbound BGP messages.

Command Modes

EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To remove all configured debug commands for BGP, enter the `no debug ip bgp` command.

debug ip bgp keepalives

Display information about BGP keepalive messages.

Syntax

```
debug ip bgp [ip-address | peer-group peer-group-name]
keepalives [in | out]
```

To disable debugging, use the `no debug ip bgp [ip-address | peer-group peer-group-name] keepalives [in | out]` command.

Parameters

ip-address	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
peer-group *peer-group-name*	(OPTIONAL) Enter the keyword `peer-group` then the name of the peer group.
in	(OPTIONAL) Enter the keyword `in` to view only inbound keepalive messages.
out	(OPTIONAL) Enter the keyword `out` to view only outbound keepalive messages.

Command Modes

EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information	To remove all configured debug commands for BGP, enter the `no debug ip bgp` command.

debug ip bgp notifications

Allows you to view information about BGP notifications received from neighbors.

Syntax

```
debug ip bgp [ip-address | peer-group peer-group-name]
notifications [in | out]
```

To disable debugging, use the `no debug ip bgp [ip-address | peer-group peer-group-name] notifications [in | out]` command.

Parameters

ip-address	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
peer-group *peer-group-name*	(OPTIONAL) Enter the keyword `peer-group` then the name of the peer group.
in	(OPTIONAL) Enter the keyword `in` to view BGP notifications received from neighbors.
out	(OPTIONAL) Enter the keyword `out` to view BGP notifications sent to neighbors

Command Modes

EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To remove all configured debug commands for BGP, enter the `no debug ip bgp` command.

debug ip bgp soft-reconfiguration

Enable soft-reconfiguration debug.

Syntax

```
debug ip bgp {ip-address | peer-group-name} soft-
reconfiguration
```

To disable, use the `no debug ip bgp {ip-address | peer-group-name} soft-reconfiguration` command.

Parameters

ip-address	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	(OPTIONAL) Enter the name of the peer group to disable or enable all routers within the peer group..

Defaults Disabled

Command Modes EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information This command turns on BGP soft-reconfiguration inbound debugging. If no neighbor is specified, debug turns on for all neighbors.

debug ip bgp updates

Allows you to view information about BGP updates.

Syntax `debug ip bgp updates [in | out | prefix-list prefix-list-name]`

To disable debugging, use the `no debug ip bgp [`*`ip-address`*` | peer-group `*`peer-group-name`*`] updates [in | out]` command.

Parameters

in	(OPTIONAL) Enter the keyword `in` to view only BGP updates received from neighbors.
out	(OPTIONAL) Enter the keyword `out` to view only BGP updates sent to neighbors.
prefix-list *prefix-list-name*	(OPTIONAL) Enter the keyword `prefix-list` then the name of an established prefix list. If the prefix list is not configured, the default is **permit** (to allow all routes).
ip-address	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	(OPTIONAL) Enter the name of the peer group to disable or enable all routers within the peer group.

Command Modes EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information	To remove all configured debug commands for BGP, enter the `no debug ip bgp` command.

default-metric

Allows you to change the metric of redistributed routes to locally originated routes. Use this command with the `redistribute` command.

Syntax	`default-metric *number*` To return to the default setting, use the `no default-metric` command.

Parameters

number	Enter a number as the metric to be assigned to routes from other protocols. The range is from 1 to 4294967295.

Defaults	**0**
Command Modes	ROUTER BGP

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information	The `default-metric` command in BGP sets the value of the BGP MULTI_EXIT_DISC (MED) attribute for redistributed routes only.
Related Commands	bgp always-compare-med — enables comparison of all BGP MED attributes. redistribute — redistributes routes from other routing protocols into BGP.

description

Enter a description of the BGP routing protocol

Syntax	`description {*description*}` To remove the description, use the `no description {*description*}` command.

Parameters

description	Enter a description to identify the BGP protocol (80 characters maximum).

Defaults	none

Command Modes

ROUTER BGP

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

router bgp — enters ROUTER mode on the switch.

max-paths

Configure the maximum number of parallel routes (multipath support) BGP supports.

Syntax

`max-paths {ebgp | ibgp} number`

To return to the default values, enter the `no maximum-paths` command.

Parameters

ebgp	Enter the keyword `ebgp` to enable multipath support for External BGP routes.
ibgp	Enter the keyword `ibgp` to enable multipath support for Internal BGP routes.
number	Enter a number as the maximum number of parallel paths. The range is from 2 to 64.

Defaults

none

Command Modes

ROUTER BGP

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

If you enable this command, use the `clear ip bgp *` command to recompute the best path.

neighbor activate

This command allows the specified neighbor/peer group to be enabled for the current AFI/SAFI (Address Family Identifier/Subsequent Address Family Identifier).

Syntax

`neighbor [ip-address | peer-group-name] activate`

To disable, use the `no neighbor [ip-address | peer-group-name] activate` command.

Parameters

ip-address	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	(OPTIONAL) Enter the name of the peer group.
activate	Enter the keyword `activate` to enable the neighbor/peer group in the new AFI/SAFI.

Defaults

Disabled

Command Modes

CONFIGURATION-ROUTER-BGP-ADDRESS FAMILY

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

By default, when you create a neighbor/peer group configuration in the Router BGP context, this enables IPv4/Unicast AFI/SAFI. When you use `activate` in the new context, the neighbor/peer group enables for AFI/SAFI.

neighbor add-path

This command allows the specified neighbor/peer group to send/receive multiple path advertisements.

Syntax

```
neighbor [ip-address | peer-group-name] add-path [send |
receive | both] count
```

Parameters

ip-address	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	(OPTIONAL) Enter the name of the peer group.
send	Enter the keyword `send` to indicate that the system sends multiple paths to peers.
receive	Enter the keyword `receive` to indicate that the system accepts multiple paths from peers.
both	Enter the keyword `both` to indicate that the system sends and accepts multiple paths from peers.
count	Enter the number paths supported. The range is from 2 to 64.

Defaults

none

Command Modes

CONFIGURATION-ROUTER-BGP-ADDRESS FAMILY

Command History	Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

bgp add-path — allows the advertisement of multiple paths for the same address prefix without the new paths implicitly replacing any previous ones.

neighbor advertisement-interval

Set the advertisement interval between BGP neighbors or within a BGP peer group.

Syntax

`neighbor {ip-address | peer-group-name} advertisement-interval seconds`

To return to the default value, use the `no neighbor {ip-address | peer-group-name} advertisement-interval` command.

Parameters

ip-address	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group to set the advertisement interval for all routers in the peer group.
seconds	Enter a number as the time interval, in seconds, between BGP advertisements. The range is from 0 to 600 seconds. The default is **5 seconds** for internal BGP peers and **30 seconds** for external BGP peers.

Defaults

- seconds = **5 seconds** (internal peers)
- seconds = **30 seconds** (external peers)

Command Modes

ROUTER BGP

Command History	Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

neighbor advertisement-start

To send BGP routing updates, set the minimum interval before starting.

Syntax

`neighbor {ip-address} advertisement-start seconds`

To return to the default value, use the `no neighbor {ip-address} advertisement-start` command.

Parameters	*ip-address*	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
	seconds	Enter a number as the time interval, in seconds, before BGP route updates are sent. The range is from 0 to 3600 seconds.

Defaults	none	
Command Modes	ROUTER BGP	
Command History	Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

neighbor allowas-in

Set the number of times an AS number can occur in the AS path.

Syntax `neighbor {ip-address | peer-group-name} allowas-in number`

To return to the default value, use the `no neighbor {ip-address | peer-group-name} allowas-in` command.

Parameters	*ip-address*	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
	peer-group-name	Enter the name of the peer group to set the advertisement interval for all routers in the peer group.
	number	Enter a number of times to allow this neighbor ID to use the AS path. The range is from 1 to 10.

Defaults	Not configured.	
Command Modes	ROUTER BGP	
Command History	Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	bgp four-octet-as-support — enables 4-byte support for the BGP process.	

neighbor default-originate

Inject the default route to a BGP peer or neighbor.

Syntax

`neighbor {ip-address | peer-group-name} default-originate [route-map map-name]`

To remove a default route, use the `no neighbor {ip-address | peer-group-name} default-originate` command.

Parameters

ip-address	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group to set the default route of all routers in that peer group.
route-map *map-name*	(OPTIONAL) Enter the keyword `route-map` then the name of a configured route map.

Defaults

Not configured.

Command Modes

ROUTER BGP

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

If you apply a route map to a BGP peer or neighbor with the `neighbor default-originate` command configured, the software does not apply the set filters in the route map to that BGP peer or neighbor.

neighbor description

Assign a character string describing the neighbor or group of neighbors (peer group).

Syntax

`neighbor {ip-address | peer-group-name} description text`

To delete a description, use the `no neighbor {ip-address | peer-group-name} description` command.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group.
text	Enter a continuous text string up to 80 characters.

Defaults

Not configured.

Command Modes

ROUTER BGP

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

neighbor distribute-list

Distribute BGP information via an established prefix list.

Syntax

`neighbor {`*`ip-address`*` | `*`peer-group-name`*`} distribute-list `*`prefix-list-name`*` {in | out}`

To delete a neighbor distribution list, use the `no neighbor {`*`ip-address`*` | `*`peer-group-name`*`} distribute-list `*`prefix-list-name`*` {in | out}` command.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group to apply the distribute list filter to all routers in the peer group.
prefix-list-name	Enter the name of an established prefix list. If the prefix list is not configured, the default is **permit** (to allow all routes).
in	Enter the keyword `in` to distribute only inbound traffic.
out	Enter the keyword `out` to distribute only outbound traffic.

Defaults

Not configured.

Command Modes

ROUTER BGP

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Other BGP filtering commands include: `neighbor filter-list`, `ip as-path access-list`, and `neighbor route-map`.

Related Commands

neighbor route-map — assigns a route map to a neighbor or peer group.

neighbor ebgp-multihop

Attempt and accept BGP connections to external peers on networks that are not directly connected.

Syntax	`neighbor {ip-address | peer-group-name} ebgp-multihop [ttl]` To disallow and disconnect connections, use the `no neighbor {ip-address | peer-group-name} ebgp-multihop` command.
Parameters	

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group.
ttl	(OPTIONAL) Enter the number of hops as the Time to Live (ttl) value. The range is from 1 to 255. The default is **255**.

Defaults	Disabled.
Command Modes	ROUTER BGP
Command History	Version 9.2(0.0) — Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	To prevent loops, the `neighbor ebgp-multihop` command does not install the default routes of the multihop peer. Networks not directly connected are not considered valid for best-path selection.

neighbor fall-over

Enable or disable fast fall-over for BGP neighbors.

Syntax	`neighbor {ipv4-address | peer-group-name} fall-over` To disable, use the `no neighbor {ipv4-address | peer-group-name} fall-over` command.
Parameters	

ipv4-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group.

Defaults	Disabled.
Command Modes	ROUTER BGP

Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	When you enable failover, BGP keeps track of IP or IPv6 ability to reach the peer remote address and the peer local address. Whenever either address becomes unreachable (for example, no active route exists in the routing table for the peer IP or IPv6 destination/local address), BGP brings down the session with the peer.
Related Commands	show ip bgp neighbors — displays information on the BGP neighbors.

neighbor graceful-restart

Enable graceful restart on a BGP neighbor.

Syntax

```
neighbor {ip-address | peer-group-name} graceful-restart
[restart-time seconds] [stale-path-time seconds] [role
receiver-only]
```

To return to the default, enter the `no bgp graceful-restart` command.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group to apply the filter to all routers in the peer group.
restart-time *seconds*	Enter the keyword `restart-time` then the maximum number of seconds to restart and bring-up all the peers. The range is from 1 to 3600 seconds. The default is **120 seconds**.
stale-path-time *seconds*	Enter the keyword `stale-path-time` then the maximum number of seconds to wait before restarting a peer's stale paths. The default is **360 seconds**.
role receiver-only	Enter the keyword `role receiver-only` to designate the local router to support graceful restart as a receiver only.

Defaults	as above
Command Modes	ROUTER BGP
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	This feature advertises to BGP neighbors through a capability advertisement. In Receiver Only mode, BGP saves the advertised routes of peers that support this capability when they restart.

neighbor local-as

To accept external routes from neighbors with a local AS number in the AS number path, configure Internal BGP (IBGP) routers.

Syntax	`neighbor {`*`ip-address`*`	`*`peer-group-name`*`} local-as `*`as-number`*` [no-prepend]` To return to the default value, use the `no neighbor {`*`ip-address`*`	`*`peer-group-name`*`} local-as` command.
Parameters	

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group to set the advertisement interval for all routers in the peer group.
as-number	Enter the AS number to reset all neighbors belonging to that AS. The range is from 0 to 65535 (2 byte), from 1 to 4294967295 (4 byte) or from 0.1 to 65535.65535 (dotted format).
no prepend	Specifies that local AS values do not prepend to announcements from the neighbor.

Defaults	Not configured.
Command Modes	ROUTER BGP
Command History	Version 9.2(0.0) — Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	bgp four-octet-as-support — enables 4-byte support for the BGP process.

neighbor maximum-prefix

Control the number of network prefixes received.

Syntax	`neighbor {`*`ip-address`*`	`*`peer-group-name`*`} maximum-prefix `*`maximum`*` [`*`threshold`*`] [warning-only]` To return to the default values, use the `no neighbor {`*`ip-address`*`	`*`peer-group-name`*`} maximum-prefix `*`maximum`* command.
Parameters	

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group.

maximum	Enter a number as the maximum number of prefixes allowed for this BGP router. The range is from 1 to 4294967295.
threshold	(OPTIONAL) Enter a number to be used as a percentage of the maximum value. When the number of prefixes reaches this percentage of the maximum value, the software sends a message. The range is from 1 to 100 percent. The default is **75**.
warning-only	(OPTIONAL) Enter the keyword `warning-only` to set the router to send a log message when the maximum value is reached. If this parameter is not set, the router stops peering when the maximum number of prefixes is reached.

Defaults

threshold = **75**

Command Modes

ROUTER BGP

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

If you configure the `neighbor maximum-prefix` command and the neighbor receives more prefixes than the `neighbor maximum-prefix` command configuration allows, the neighbor goes down and the `show ip bgp summary` command displays (prfxd) in the State/PfxRcd column for that neighbor. The neighbor remains down until you enter the `clear ip bgp` command for the neighbor or the peer group to which the neighbor belongs or you enter the `neighbor shutdown` and `neighbor no shutdown` commands.

Related Commands

show ip bgp summary — displays the current BGP configuration.

neighbor password

Enable message digest 5 (MD5) authentication on the TCP connection between two neighbors.

Syntax

`neighbor {ip-address | peer-group-name} password [encryption-type] password`

To delete a password, use the `no neighbor {ip-address | peer-group-name} password` command.

Parameters

ip-address	Enter the IP address of the router to be included in the peer group.
peer-group-name	Enter the name of a configured peer group.
encryption-type	(OPTIONAL) Enter `7` as the encryption type for the password entered. `7` means that the password is encrypted and hidden.

password	Enter a text string up to 80 characters long. The first character of the password must be a letter. You cannot use spaces in the password.

Defaults Not configured.

Command Modes ROUTER BGP

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Configure the same password on both BGP peers or a connection does not occur. When you configure MD5 authentication between two BGP peers, each segment of the TCP connection between them is verified and the MD5 digest is checked on every segment sent on the TCP connection.

Configuring a password for a neighbor causes an existing session to be torn down and a new one established.

If you specify a BGP peer group by using the `peer-group-name` parameter, all the members of the peer group inherit the characteristic configured with this command.

If you configure a password on one neighbor, but you have not configured a password for the neighboring router, the following message appears on the console while the routers attempt to establish a BGP session between them:

```
%RPM0-P:RP1 %KERN-6-INT: No BGP MD5 from [peer's IP address]
:179 to [local router's IP address]:65524
```

Also, if you configure different passwords on the two routers, the following message appears on the console:

```
%RPM0-P:RP1 %KERN-6-INT: BGP MD5 password mismatch from
[peer's IP address] : 11502 to [local router's IP address] :179
```

neighbor peer-group (assigning peers)

Allows you to assign one peer to an existing peer group.

Syntax

`neighbor ip-address peer-group peer-group-name`

To delete a peer from a peer group, use the `no neighbor ip-address peer-group peer-group-name` command.

Parameters

ip-address	Enter the IP address of the router to be included in the peer group.

peer-group-name	Enter the name of a configured peer group.

Defaults Not configured.

Command Modes ROUTER BGP

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

You can assign up to 256 peers to one peer group.

When you add a peer to a peer group, it inherits all the peer group's configured parameters. A peer cannot become part of a peer group if any of the following commands are configured on the peer:

- neighbor advertisement-interval
- neighbor distribute-list
- neighbor route-map
- neighbor route-reflector-client
- neighbor shutdown

A neighbor may keep its configuration after it was added to a peer group if the neighbor's configuration is more specific than the peer group's, and the neighbor's configuration does not affect outgoing updates.

A peer group must exist before you add a peer to it. If the peer group is disabled (shutdown) the peers within the group are also disabled (shutdown).

Related Commands

clear ip bgp — resets BGP sessions.

neighbor peer-group (creating group) — creates a peer group.

show ip bgp peer-group — views BGP peers.

show ip bgp neighbors — views BGP neighbors configurations.

neighbor peer-group (creating group)

Allows you to create a peer group and assign it a name.

Syntax `neighbor peer-group-name peer-group`

To delete a peer group, use the `no neighbor peer-group-name peer-group` command.

Parameters	*peer-group-name*	Enter a text string up to 16 characters long as the name of the peer group.
Defaults	Not configured.	
Command Modes	ROUTER BGP	
Command History	Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	When you create a peer group, it is disabled (Shut mode).	
Related Commands	neighbor peer-group (assigning peers) — assigns routers to a peer group. neighbor remote-as — assigns a indirectly connected AS to a neighbor or peer group. neighbor shutdown — disables a peer or peer group.	

neighbor peer-group passive

Enable passive peering on a BGP peer group, that is, the peer group does not send an OPEN message, but responds to one.

Syntax

```
neighbor peer-group-name peer-group passive [limit sessions]
```

To delete a passive peer-group, use the `no neighbor peer-group-name peer-group passive` command.

Parameters	*peer-group-name*	Enter a text string up to 16 characters long as the name of the peer group.
	limit	(Optional) Enter the keyword `limit` to constrain the numbers of sessions for this peer-group. The range is from 2 to 256. The default is **256**.
Defaults	Not configured.	
Command Modes	ROUTER BGP	
Command History	Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	After you configure a peer group as passive, assign it a subnet using the `neighbor soft-reconfiguration inbound` command.	

For passive eBGP limits, the Remote AS must be different from the AS for this neighbor.

Related Commands	neighbor soft-reconfiguration inbound — assigns a subnet to a dynamically configured BGP neighbor. neighbor remote-as — assigns an indirectly connected AS to a neighbor or peer group.

neighbor remote-as

Create and specify the remote peer to the BGP neighbor.

Syntax

`neighbor {ip-address | peer-group-name} remote-as number`

To delete a remote AS entry, use the `no neighbor {ip-address | peer-group-name} remote-as number` command.

Parameters

ip-address	Enter the IP address of the neighbor to enter the remote AS in its routing table.
peer-group-name	Enter the name of the peer group to enter the remote AS into routing tables of all routers within the peer group.
number	Enter a number of the AS. The range is from 0 to 65535 (2 byte) or from 1 to 4294967295 (4 byte).

Defaults

Not configured.

Command Modes

ROUTER BGP

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To accept 4-byte formats before entering a 4 byte AS Number, configure your system. If the `number` parameter is the same as the AS number used in the `router bgp` command, the remote AS entry in the neighbor is considered an internal BGP peer entry.

This command creates a peer and the newly created peer is disabled (Shutdown).

Related Commands

router bgp — enters ROUTER BGP mode and configures routes in an AS.

bgp four-octet-as-support — enables 4-byte support for the BGP process.

neighbor remove-private-as

Remove private AS numbers from the AS-PATH of outgoing updates.

Syntax	`neighbor {ip-address	peer-group-name} remove-private-as` To return to the default, use the `no neighbor {ip-address	peer-group-name} remove-private-as` command.
Parameters	*ip-address*: Enter the IP address of the neighbor to remove the private AS numbers. *peer-group-name*: Enter the name of the peer group to remove the private AS numbers.
Defaults	Disabled (that is, private AS number are not removed).
Command Modes	ROUTER BGP
Command History	Version 9.2(0.0): Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	Applies to EBGP neighbors only. Configure your system to accept 4-byte formats before entering a 4 byte AS Number. If the AS-PATH contains both public and private AS number or contains AS numbers of an EBGP neighbor, the private AS numbers are not removed. If a confederation contains private AS numbers in its AS-PATH, the software removes the private AS numbers only if they follow the confederation numbers in the AS path. Private AS numbers are from 64512 to 65535 (2 byte).

neighbor route-map

Apply an established route map to either incoming or outbound routes of a BGP neighbor or peer group.

Syntax	`neighbor {ip-address	peer-group-name} route-map map-name {in	out}` To remove the route map, use the `no neighbor {ip-address	peer-group-name} route-map map-name {in	out}` command.
Parameters	*ip-address*: Enter the IP address of the neighbor in dotted decimal format.

peer-group-name	Enter the name of the peer group.
map-name	Enter the name of an established route map. If the Route map is not configured, the default is **deny** (to drop all routes).
in	Enter the keyword `in` to filter inbound routes.
out	Enter the keyword `out` to filter outbound routes.

Defaults

Not configured.

Command Modes

ROUTER BGP

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

When you apply a route map to outbound routes, only routes that match at least one section of the route map are permitted.

If you identify a peer group by name, the peers in that peer group inherit the characteristics in the Route map used in this command. If you identify a peer by IP address, the Route map overwrites either the inbound or outbound policies on that peer.

neighbor route-reflector-client

Configure the router as a route reflector and the specified neighbors as members of the cluster.

Syntax

```
neighbor {ip-address | peer-group-name} route-reflector-client
```

To remove one or more neighbors from a cluster, use the `no neighbor {ip-address | peer-group-name} route-reflector-client` command. If you delete all members of a cluster, you also delete the route-reflector configuration on the router.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group. All routers in the peer group receive routes from a route reflector.

Defaults

Not configured.

Command Modes	ROUTER BGP
Command History	Version 9.2(0.0) — Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	A route reflector reflects routes to the neighbors assigned to the cluster. Neighbors in the cluster do not need not to be fully meshed. By default, when you use `no route reflector`, the internal BGP (IBGP) speakers in the network must be fully meshed. The first time you enter this command, the router configures as a route reflector and the specified BGP neighbors configure as clients in the route-reflector cluster. When you remove all clients of a route reflector using the `no neighbor route-reflector-client` command, the router no longer functions as a route reflector. If the clients of a route reflector are fully meshed, you can configure the route reflector to not reflect routes to specified clients by using the `no bgp client-to-client reflection` command.
Related Commands	bgp client-to-client reflection — enables route reflection between the route reflector and the clients.

neighbor shutdown

Disable a BGP neighbor or peer group.

Syntax	`neighbor {ip-address | peer-group-name} shutdown` To enable a disabled neighbor or peer group, use the `neighbor {ip-address | peer-group-name} no shutdown` command.
Parameters	*ip-address* — Enter the IP address of the neighbor in dotted decimal format. *peer-group-name* — Enter the name of the peer group to disable or enable all routers within the peer group.
Defaults	Enabled (that is, BGP neighbors and peer groups are disabled.)
Command Modes	ROUTER BGP
Command History	Version 9.2(0.0) — Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information	Peers that are enabled within a peer group are disabled when their peer group is disabled. The `neighbor shutdown` command terminates all BGP sessions on the BGP neighbor or BGP peer group. Use this command with caution as it terminates the specified BGP sessions. When a neighbor or peer group is shut down, use the `show ip bgp summary` command to confirm its status.
Related Commands	show ip bgp summary — displays the current BGP configuration. show ip bgp neighbors — displays the current BGP neighbors.

neighbor soft-reconfiguration inbound

Enable soft-reconfiguration for BGP.

Syntax

`neighbor {`*`ip-address`*` | `*`peer-group-name`*`} soft-reconfiguration inbound`

To disable, use the `no neighbor {`*`ip-address`*` | `*`peer-group-name`*`} soft-reconfiguration inbound` command.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group to disable or enable all routers within the peer group.

Defaults	Disabled
Command Modes	ROUTER BGP

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

This command enables soft-reconfiguration for the BGP neighbor specified. BGP stores all the updates the neighbor receives but does not reset the peer-session.

⚠ **CAUTION: Inbound update storage is a memory-intensive operation. The entire BGP update database from the neighbor is stored in memory regardless of the inbound policy results applied on the neighbor.**

NOTE: This command is supported in BGP Router Configuration mode for IPv4 Unicast address only.

Related Commands

show ip bgp neighbors — displays routes received by a neighbor.

neighbor timers

Set keepalive and hold time timers for a BGP neighbor or a peer group.

Syntax

`neighbor {ip-address | peer-group-name} timers keepalive holdtime`

To return to the default values, use the `no neighbor {ip-address | peer-group-name} timers` command.

Parameters

ip-address	Enter the IP address of the peer router in dotted decimal format.
peer-group-name	Enter the name of the peer group to set the timers for all routers within the peer group.
keepalive	Enter a number for the time interval, in seconds, between keepalive messages sent to the neighbor routers. The range is from 1 to 65535. The default is **60 seconds**.
holdtime	Enter a number for the time interval, in seconds, between the last keepalive message and declaring the router dead. The range is from 3 to 65535. The default is **180 seconds**.

Defaults

- keepalive = **60 seconds**
- holdtime = **180 seconds**

Command Modes

ROUTER BGP

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Timer values configured with the `neighbor timers` command override the timer values configured with any other command.

When two neighbors, configured with different `keepalive` and `holdtime` values, negotiate for new values, the resulting values are as follows:

- the lower of the `holdtime` value is the new `holdtime` value, and
- whichever is the lower value; one-third of the new `holdtime` value, or the configured `keepalive` value, is the new keepalive value.

neighbor update-source

Enable the software to use Loopback interfaces for TCP connections for BGP sessions.

Syntax

`neighbor {ip-address | peer-group-name} update-source interface`

To use the closest interface, use the `no neighbor {ip-address | peer-group-name} update-source interface` command.

Parameters

ip-address	Enter the IP address of the peer router in dotted decimal format.
peer-group-name	Enter the name of the peer group to disable all routers within the peer group.
interface	Enter the keyword `loopback` then a number of the Loopback interface. The range is from 0 to 16383.

Defaults Not configured.

Command Modes ROUTER BGP

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information Loopback interfaces are up constantly and the BGP session may need one interface constantly up to stabilize the session. The `neighbor update-source` command is not necessary for directly connected internal BGP sessions.

neighbor weight

Assign a weight to the neighbor connection, which is used to determine the best path.

Syntax `neighbor {ip-address | peer-group-name} weight weight`

To remove a weight value, use the `no neighbor {ip-address | peer-group-name} weight` command.

Parameters

ip-address	Enter the IP address of the peer router in dotted decimal format.
peer-group-name	Enter the name of the peer group to disable all routers within the peer group.
weight	Enter a number as the weight. The range is from 0 to 65535. The default is **0**.

Defaults **0**

Command Modes ROUTER BGP

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

In the system best path selection process, the path with the highest weight value is preferred.

NOTE: In the system best-path selection process, the path with the highest weight value is preferred.

If you configure the `set weight` command in a route map applied to this neighbor, the weight set in that command overrides the weight set in the `neighbor weight` command.

network

Specify the networks for the BGP process and enter them in the BGP routing table.

Syntax

`network ip-address mask [route-map map-name]`

To remove a network, use the `no network ip-address mask [route-map map-name]` command.

Parameters

ip-address	Enter an IP address in dotted decimal format of the network.
mask	Enter the mask of the IP address in the slash prefix length format (for example, /24). The mask appears in command outputs in dotted decimal format (A.B.C.D).
route-map *map-name*	(OPTIONAL) Enter the keyword `route-map` then the name of an established route map. Only the following ROUTE-MAP mode commands are supported: • match ip address • set metric • set tag If the route map is not configured, the default is **deny** (to drop all routes).

Defaults

Not configured.

Command Modes

ROUTER BGP

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information	The system software resolves the network address the `network` command configures with the routes in the main routing table to ensure that the networks are reachable using non-BGP routes and non-default routes.
Related Commands	redistribute — redistributes routes into BGP.

network backdoor

Specify this IGP route as the preferred route.

Syntax

`network` *`ip-address mask`* `backdoor`

To remove a network, use the `no network` *`ip-address mask`* `backdoor` command.

Parameters

ip-address	Enter an IP address in dotted decimal format of the network.
mask	Enter the mask of the IP address in the slash prefix length format (for example, /24). The mask appears in command outputs in dotted decimal format (A.B.C.D).

Defaults	Not configured.
Command Modes	ROUTER BGP

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Although the system does not generate a route due to the backdoor config, there is an option for injecting/sourcing a local route in the presence of network backdoor config on a learned route.

redistribute

Redistribute routes into BGP.

Syntax

`redistribute {connected | static} [route-map` *`map-name`*`]`

To disable redistribution, use the `no redistribution {connected | static}` command.

Parameters

connected	Enter the keyword `connected` to redistribute routes from physically connected interfaces.

static	Enter the keyword `static` to redistribute manually configured routes. These routes are treated as incomplete routes.
route-map *map-name*	(OPTIONAL) Enter the keyword `route-map` then the name of an established route map. Only the following ROUTE-MAP mode commands are supported: • match ip address • set metric • set tag If the route map is not configured, the default is **deny** (to drop all routes).

Defaults

Not configured.

Command Modes

ROUTER BGP

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

With the Dell Networking OS version 8.3.1.0 and later, you can use the `redistribute` command to advertise the IGP cost as the MED on redistributed routes. When you set the route-map with metric-type internal and applied outbound to an EBGP peer/peer-group, the advertised routes corresponding to those peer/peer-groups have the IGP cost set as **MED**.

If you do not configure the `default-metric` command, in addition to the `redistribute` command, or there is no route map to set the metric, the metric for redistributed static and connected is “0”.

To redistribute the default route (0.0.0.0/0), configure the `neighbor default-originate` command.

Related Commands

neighbor default-originate — injects the default route.

redistribute ospf

Redistribute OSPF routes into BGP.

Syntax

```
redistribute ospf process-id [[match external {1 | 2}] [match
internal]] [route-map map-name]
```

To stop redistribution of OSPF routes, use the `no redistribute ospf` *`process-id`* command.

Parameters

process-id	Enter the number of the OSPF process. The range is from 1 to 65535.
match external {1 | 2}	(OPTIONAL) Enter the keywords `match external` to redistribute OSPF external routes. You can specify `1` or `2` to redistribute those routes only.
match internal	(OPTIONAL) Enter the keywords `match internal` to redistribute OSPF internal routes only.
route-map *map-name*	(OPTIONAL) Enter the keywords `route-map` then the name of a configured route map.

Defaults Not configured.

Command Modes ROUTER BGP

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

With the Dell Networking OS version 8.3.1.0 and later, you can use the `redistribute` command to advertise the IGP cost as the MED on redistributed routes. When you set the route-map with metric-type internal and apply outbound to an EBGP peer/peer-group, the advertised routes corresponding to those peer/peer-groups have the IGP cost set as **MED**.

When you enter the `redistribute isis` *`process-id`* command without any other parameters, the system redistributes all OSPF internal routes, external type 1 routes, and external type 2 routes. RFC does not support this feature.

router bgp

To configure and enable BGP, enter ROUTER BGP mode.

Syntax

```
router bgp as-number
```

To disable BGP, use the `no router bgp` *`as-number`* command.

Parameters

as-number	Enter the AS number. The range is from 1 to 65535 (2 byte), from 1 to 4294967295 (4 byte), or from 0.1 to 65535.65535 (dotted format).

Defaults Not enabled.

Command Modes

CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

At least one interface must be in Layer 3 mode for the `router bgp` command to be accepted. If no interfaces are enabled for Layer 3, an error message appears:

```
% Error: No router id
configured
```

Example

```
Dell(conf)#router bgp 3
Dell(conf-router_bgp)#
```

show capture bgp-pdu neighbor

Display BGP packet capture information for an IPv4 address on the system.

Syntax

`show capture bgp-pdu neighbor` *`ipv4-address`*

Parameters

ipv4-address	Enter the IPv4 address (in dotted decimal format) of the BGP address to display packet information for that address.

Command Modes

EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell(conf-router_bgp)#show capture bgp-pdu neighbor 20.20.20.2

Incoming packet capture enabled for BGP neighbor 20.20.20.2
Available buffer size 40958758, 26 packet(s) captured using
680 bytes
  PDU[1] : len 101, captured 00:34:51 ago
    ffffffff ffffffff ffffffff ffffffff 00650100 00000013
00000000
00000000 419ef06c 00000000
    00000000 00000000 00000000 00000000 0181a1e4 0181a25c
41af92c0
00000000 00000000 00000000
    00000000 00000001 0181a1e4 0181a25c 41af9400 00000000
  PDU[2] : len 19, captured 00:34:51 ago
    ffffffff ffffffff ffffffff ffffffff 00130400
  PDU[3] : len 19, captured 00:34:51 ago
    ffffffff ffffffff ffffffff ffffffff 00130400
 [. . .]

Outgoing packet capture enabled for BGP neighbor 20.20.20.2
Available buffer size 40958758, 27 packet(s) captured using
562 bytes
  PDU[1] : len 41, captured 00:34:52 ago
    ffffffff ffffffff ffffffff ffffffff 00290104 000100b4
14141401
```

```
0c020a01 04000100 01020080
    00000000
  PDU[2] : len 19, captured 00:34:51 ago
    ffffffff ffffffff ffffffff ffffffff 00130400
  PDU[3] : len 19, captured 00:34:50 ago
    ffffffff ffffffff ffffffff ffffffff 00130400
 [. . .]
Dell#
```

Related Commands	capture bgp-pdu max-buffer-size — specifies a size for the capture buffer.

show config

View the current ROUTER BGP configuration.

Syntax `show config`

Command Modes ROUTER BGP

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell(conf-router_bgp)#show config
!
router bgp 45
 neighbor suzanne peer-group
 neighbor suzanne no shutdown
 neighbor sara peer-group
 neighbor sara shutdown
 neighbor 13.14.15.20 peer-group suzanne
 neighbor 13.14.15.20 shutdown
 neighbor 123.34.55.123 peer-group suzanne
 neighbor 123.34.55.123 shutdown
Dell(conf-router_bgp)#
```

Related Commands	capture bgp-pdu max-buffer-size — specifies a size for the capture buffer.

show ip bgp

View the current BGP IPv4 routing table for the system.

Syntax `show ip bgp [ipv4 unicast] [network [network-mask] [longer-prefixes]]`

Parameters

ipv4 unicast	(OPTIONAL) Enter the keywords `ipv4 unicast` to view information only related to ipv4 unicast routes.

network	(OPTIONAL) Enter the network address (in dotted decimal format) of the BGP network to view information only on that network.
network-mask	(OPTIONAL) Enter the network mask (in slash prefix format) of the BGP network address.
longer-prefixes	(OPTIONAL) Enter the keywords `longer-prefixes` to view all routes with a common prefix.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

When you enable the `bgp non-deterministic-med` command, the `show ip bgp` command output for a BGP route does not list the INACTIVE reason.

The following describes the `show ip bgp` command shown in the following example.

Field	Description
Network	Displays the destination network prefix of each BGP route.
Next Hop	Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then local routes exist in the routing table.
Metric	Displays the BGP route's metric, if assigned.
LocPrf	Displays the BGP LOCAL_PREF attribute for the route.
Weight	Displays the route's weight.
Path	Lists all the ASs the route passed through to reach the destination network.

Example

```
Dell>show ip bgp
BGP table version is 847562, local router ID is 63.114.8.131
Status codes: s suppressed, d damped, h history, * valid, >
best
Path source: I - internal, a - aggregate, c - confed-external,
r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network         Next Hop   Metric LocPrf Weight Path
*>  0.0.0.0/0      63.114.8.33                  0 18508 i
*   3.0.0.0/8      63.114.8.33                  0 18508 209
701 80 i
*>                 63.114.8.33                  0 18508 701 80
i
*>  3.3.0.0/16     0.0.0.0        22        32768 ?
                   63.114.8.35                  0 18508 ?
*>  4.0.0.0/8      63.114.8.33                  0 18508 701 1 i
*>  4.2.49.12/30   63.114.8.33                  0 18508 209 i
*   4.17.250.0/24  63.114.8.33                  0 18508 209
```

```
1239 13716 i
*>  63.114.8.33                                    0 18508 701
1239 13716 i
*   4.21.132.0/23  63.114.8.33                     0 18508 209
6461 16422 i
*>                 63.114.8.33                     0 18508 701
6461 16422 i
*>  4.24.118.16/30 63.114.8.33                     0 18508 209 i
*>  4.24.145.0/30  63.114.8.33                     0 18508 209 i
*>  4.24.187.12/30 63.114.8.33                     0 18508 209 i
*>  4.24.202.0/30  63.114.8.33                     0 18508 209 i
*>  4.25.88.0/30   63.114.8.33                     0 18508 209
3561 3908 i
*>  5.0.0.0/9      63.114.8.33     0               0 18508 ?
*>  5.0.0.0/10     63.114.8.33     0               0 18508 ?
*>  5.0.0.0/11     63.114.8.33     0               0 18508 ?
--More--
```

Related Commands

show ip bgp community — views the BGP communities.

neighbor maximum-prefix — controls the number of network prefixes received.

show ip bgp cluster-list

View BGP neighbors in a specific cluster.

Syntax `show ip bgp [ipv4 unicast] cluster-list [cluster-id]`

Parameters

ipv4 unicast	(OPTIONAL) Enter the keywords `ipv4 unicast` to view information only related to ipv4 unicast routes.
cluster-id	(OPTIONAL) Enter the cluster id in dotted decimal format. The range is 1 — 4294967295.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show ip bgp cluster-list` command shown in the following example.

Field	Description
Network	Displays the destination network prefix of each BGP route.
Next Hop	Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then local routes exist in the routing table.

Field	Description
Metric	Displays the BGP route's metric, if assigned.
LocPrf	Displays the BGP LOCAL_PREF attribute for the route.
Weight	Displays the route's weight.
Path	Lists all the ASs the route passed through to reach the destination network.

Example

```
Dell#show ip bgp cluster-list
BGP table version is 64444683, local router ID is 120.1.1.1
Status codes: s suppressed, d damped, h history, * valid, >
best
Path source: I - internal, a - aggregate, c - confed-external,
r - redistributed, n
- network
Origin codes: i - IGP, e - EGP, ? - incomplete

     Network          Next Hop      Metric LocPrf Weight Path
* I 10.10.10.1/32     192.68.16.1        0    100      0 i
* I                   192.68.16.1        0    100      0 i
*>I                   192.68.16.1        0    100      0 i
* I                   192.68.16.1        0    100      0 i
* I                   192.68.16.1        0    100      0 i
* I                   192.68.16.1        0    100      0 i
* I 10.19.75.5/32     192.68.16.1        0    100      0 ?
* I                   192.68.16.1        0    100      0 ?
*>I                   192.68.16.1        0    100      0 ?
* I                   192.68.16.1        0    100      0 ?
* I                   192.68.16.1        0    100      0 ?
* I                   192.68.16.1        0    100      0 ?
* I 10.30.1.0/24      192.68.16.1        0    100      0 ?
* I                   192.68.16.1        0    100      0 ?
*>I                   192.68.16.1        0    100      0 ?
* I                   192.68.16.1        0    100      0 ?
* I                   192.68.16.1        0    100      0 ?
* I                   192.68.16.1        0    100      0 ?
```

show ip bgp community

View information on all routes with Community attributes or view specific BGP community groups.

Syntax

```
show ip bgp [ipv4 unicast] community [community-number] [local-
as] [no-export] [no-advertise]
```

Parameters

ipv4 unicast	(OPTIONAL) Enter the keywords `ipv4 unicast` to view information only related to ipv4 unicast routes.
community-number	Enter the community number in AA:NN format where AA is the AS number (2 bytes) and NN is a value specific to that autonomous system.

	You can specify up to eight community numbers to view information on those community groups.
local-AS	Enter the keywords `local-AS` to view all routes with the COMMUNITY attribute of NO_EXPORT_SUBCONFED. All routes with the NO_EXPORT_SUBCONFED (0xFFFFFF03) community attribute must not be advertised to external BGP peers.
no-advertise	Enter the keywords `no-advertise` to view all routes containing the well-known community attribute of NO_ADVERTISE. All routes with the NO_ADVERTISE (0xFFFFFF02) community attribute must not be advertised to other BGP peers.
no-export	Enter the keywords `no-export` to view all routes containing the well-known community attribute of NO_EXPORT. All routes with the NO_EXPORT (0xFFFFFF01) community attribute must not be advertised outside a BGP confederation boundary.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To view the total number of COMMUNITY attributes found, use the `show ip bgp summary` command. The text line above the route table states the number of COMMUNITY attributes found.

The `show ip bgp community` command without any parameters lists BGP routes with at least one BGP community attribute and the output is the same as for the `show ip bgp` command output.

The following describes the `show ip bgp community` command shown in the following example.

Field	Description
Network	Displays the destination network prefix of each BGP route.
Next Hop	Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then local routes exist in the routing table.

Field	Description
Metric	Displays the BGP route’s metric, if assigned.
LocPrf	Displays the BGP LOCAL_PREF attribute for the route.
Weight	Displays the route’s weight.
Path	Lists all the ASs the route passed through to reach the destination network.

Example

```
Dell>show ip bgp community
BGP table version is 3762622, local router ID is 63.114.8.48
Status codes: s suppressed, d damped, h history, * valid, >
best
Path source: I - internal, a - aggregate, c - confed-external,
r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete

Network            Next Hop   Metric LocPrf Weight Path
* i 3.0.0.0/8      205.171.0.16         100    0 209 701 80 i
*>i 4.2.49.12/30   205.171.0.16         100    0 209 i
* i 4.21.132.0/23  205.171.0.16         100    0 209 6461
16422 i
*>i 4.24.118.16/3  205.171.0.16         100    0 209 i
*>i 4.24.145.0/30  205.171.0.16         100    0 209 i
*>i 4.24.187.12/30 205.171.0.16         100    0 209 i
*>i 4.24.202.0/30  205.171.0.16         100    0 209 i
*>i 4.25.88.0/30   205.171.0.16         100    0 209 3561 3908
i
*>i 6.1.0.0/16     205.171.0.16         100    0 209 7170 1455
i
*>i 6.2.0.0/22     205.171.0.16         100    0 209 7170 1455
i
*>i 6.3.0.0/18     205.171.0.16         100    0 209 7170 1455
i
*>i 6.4.0.0/16     205.171.0.16         100    0 209 7170 1455
i
*>i 6.5.0.0/19     205.171.0.16         100    0 209 7170 1455
i
*>i 6.8.0.0/20     205.171.0.16         100    0 209 7170 1455
i
*>i 6.9.0.0/20     205.171.0.16         100    0 209 7170 1455
i
*>i 6.10.0.0/15    205.171.0.16         100    0 209 7170 1455
i
*>i 6.14.0.0/15    205.171.0.16         100    0 209 7170 1455
i
*>i 6.133.0.0/21   205.171.0.16         100    0 209 7170 1455
i
*>i 6.151.0.0/1    205.171.0.16         100    0 209 7170 1455
i
--More--
```

show ip bgp community-list

View routes that a specific community list affects.

Syntax

`show ip bgp [`*`ipv4 unicast`*`] community-list `*`community-list-name`*` [exact-match]`

Parameters

ipv4 unicast	(OPTIONAL) Enter the keywords `ipv4 unicast` to view information only related to ipv4 unicast routes.
community-list-name	Enter the name of a configured IP community list (maximum 140 characters).
exact-match	Enter the keyword for an exact match of the communities.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The `show ip bgp community-list` command without any parameters lists BGP routes matching the Community List and the output is the same as for the `show ip bgp` command output.

The following describes the `show ip bgp community-list pass` command shown in the following example.

Field	Description
Network	Displays the destination network prefix of each BGP route.
Next Hop	Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then local routes exist in the routing table.
Metric	Displays the BGP route's metric, if assigned.
LocPrf	Displays the BGP LOCAL_PREF attribute for the route.
Weight	Displays the route's weight.
Path	Lists all the ASs the route passed through to reach the destination network.

Example

```
Dell#show ip bgp community-list pass
BGP table version is 0, local router ID is 10.101.15.13
Status codes: s suppressed, d damped, h history, * valid, >
best
Path source: I - internal, a - aggregate, c - confed-external,
r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
Network      Next Hop      Metric      LocPrf      Weight Path
Dell#
```

show ip bgp dampened-paths

View BGP routes that are dampened (non-active).

Syntax	`show ip bgp [ipv4 unicast] dampened-paths`
Command Modes	• EXEC • EXEC Privilege
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show ip bgp damp` command shown in the following example.

Field	Description
Network	Displays the network ID to which the route is dampened.
From	Displays the IP address of the neighbor advertising the dampened route.
Reuse	Displays the hour:minutes:seconds until the dampened route is available.
Path	Lists all the ASs the dampened route passed through to reach the destination network.

Example

```
Dell>show ip bgp dampened-paths
BGP table version is 210708, local router ID is 63.114.8.2
Status codes: s suppressed, d damped, h history, * valid, >
best
Path source: I - internal, a - aggregate, c - confed-external,
r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network      From       Reuse       Path
Dell>
```

show ip bgp detail

Display BGP internal information for the IPv4 Unicast address family.

Syntax	`show ip bgp [ipv4 unicast] detail`
Defaults	none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show ip bgp detail
Detail information for BGP Node
bgpNdP 0x41a17000 : NdTmrP 0x41a17000 : NdKATmrP 0x41a17014 :
NdTics 74857 :
NhLocAS 1 : NdState 2 : NdRPMPrim 1 : NdListSoc 13
NdAuto 1 : NdEqCost 1 : NdSync 0 : NdDefOrg 0
NdV6ListSoc 14 NdDefDid 0 : NdConfedId 0 : NdMedConfed 0 :
NdMedMissVal -1 :
NdIgnrIllId 0 : NdRRC2C 1 : NdClstId 33686273 : NdPaTblP
0x41a19088
NdASPTblP 0x41a19090 : NdCommTblP 0x41a19098 : NhOptTransTblP
0x41a190a0 :
NdRRClsTblP 0x41a190a8
NdPktPA 0 : NdLocCBP 0x41a6f000 : NdTmpPAP 0x419efc80 :
NdTmpASPAP 0x41a25000 :
NdTmpCommP 0x41a25800
NdTmpRRClP 0x41a4b000 : NdTmpOptP 0x41a4b800 : NdTmpNHP :
NdOrigPAP 0
NdOrgNHP 0 : NdModPathP 0x419efcc0 : NdModASPAP 0x41a4c000 :
NdModCommP 0x41a4c800
NdModOptP 0x41a4d000 : NdModNHP : NdComSortBufP 0x41a19110 :
NdComSortHdP
0x41a19d04 : NdUpdAFMsk 0 : AFRstSet 0x41a1a298 : NHopDfrdHdP
0x41a1a3e0 :

NumNhDfrd 0 : CfgHdrAFMsk 1
AFChkNetTmrP 0x41ee705c : AFRtDamp 0 : AlwysCmpMed 0 : LocrHld
10 : LocrRem 10 :
softReconfig 0x41a1a58c
DefMet 0 : AutoSumm 1 : NhopsP 0x41a0d100 : Starts 0 : Stops
0 : Opens 0
Closes 0 : Fails 0 : Fatals 0 : ConnExps 0 : HldExps 0 :
KeepExps 0
RxOpens 0 : RxKeeps 0 : RxUpds 0 : RxNotifs 0 : TxUpds 0 :
TxNotifs 0
BadEvts 0 : SynFails 0 : RxeCodeP 0x41a1b6b8 : RxHdrCodeP
0x41a1b6d4 : RxOpCodeP
0x41a1b6e4
RxUpdCodeP 0x41a1b704 : TxEcodeP 0x41a1b734 : TxHdrcodeP
0x41a1b750 : TxOpCodeP
0x41a1b760
TxUpdCodeP 0x41a1b780 : TrEvt 0 : LocPref 100 : tmpPathP
0x41a1b7b8 : LogNbrChgs 1
RecursiveNH 1 : PgCfgId 0 : KeepAlive 0 : HldTime 0 : DioHdl
0 : AggrValTmrP
0x41ee7024
UpdNetTmrP 0 : RedistTmrP 0x41ee7094 : PeerChgTmrP 0 :
CleanRibTmrP 0x41ee7104
PeerUpdTmrP 0x41ee70cc : DfrdNHTmrP 0x41ee7174 : DfrdRtselTmrP
0x41ee713c :
FastExtFallover 1 : FastIntFallover 0 : Enforce1stAS 1
PeerIdBitsP 0x41967120 : softOutSz 16 : RibUpdCtxCBP 0
UpdPeerCtxCBP 0 : UpdPeerCtxAFI 0 : TcpioCtxCB 0 : RedistBlk 1
NextCBPurg 1101119536 : NumPeerToPurge 0 : PeerIBGPCnt 0 :
NonDet 0 : DfrdPathSel 0
```

```
BGPRst 0 : NumGrCfg 1 : DfrdTmestmp 0 : SnmpTrps 0 :
IgnrBestPthASP 0
RstOn 1 : RstMod 1 : RstRole 2 : AFFalgs 7 : RstInt 120 :
MaxeorExtInt 361
FixedPartCrt 1 : VarParCrt 1
Packet Capture max allowed length 40960000 : current length 0

Peer Grp List
Nbr List
Confed Peer List
Address Family specific Information
AFIndex 0
NdSpFlag 0x41a190b0 : AFRttP 0x41a0d200 : NdRTMMkrP
0x41a19d28 : NdRTMAFTblVer 0 :
NdRibCtxAddr 1101110688
NdRibCtxAddrLen 255 : NdAFPrefix 0 : NdAfNLRIP 0 : NdAFNLRILen
0 : NdAFWPtrP 0
NdAFWLen 0 : NdAfNH : NdAFRedRttP 0x41a0d400 : NdRecCtxAdd
1101110868
NdRedCtxAddrLen 255 : NdAfRedMkrP 0x41a19e88 : AFAggRttP
0x41a0d600 : AfAggCtxAddr
1101111028 : AfAggrCtxAddrLen 255
AfNumAggrPfx 0 : AfNumAggrASSet 0 : AfNumSuppmap 0 :
AfNumAggrValidPfx 0 :
AfMPathRttP 0x41a0d700
MpathCtxAddr 1101111140 : MpathCtxAddrlen 255 : AfEorSet
0x41a19f98 : NumDfrdPfx 0
AfActPeerHd 0x41a1a3a4 : AfExtDist 1101112312 : AfIntDist
200 : AfLocDist 200
AfNumRRc 0 : AfRR 0 : AfNetRttP 0x41a0d300 : AfNetCtxAddr
1101112392 :
AfNetCtxAddrlen 255
AfNwCtxAddr 1101112443 : AfNwCtxAddrlen 255 : AfNetBKDrRttP
0x41a0d500 :
AfNetBKDRCnt 0 : AfDampHLife 0
AfDampReuse 0 : AfDampSupp 0 : AfDampMaxHld 0 : AfDampCeiling
0 : AfDampRmapP
```

show ip bgp extcommunity-list

View information on all routes with Extended Community attributes.

Syntax

show ip bgp [*ipv4 unicast*] extcommunity-list [*list name*]

Parameters

ipv4 unicast	(OPTIONAL) Enter the keywords `ipv4 unicast` to view information only related to ipv4 unicast routes.
list name	Enter the extended community list name you wish to view. The range is 140 characters.

Command Modes

- EXEC
- EXEC Privilege

Command History	**Version 9.2(0.0)**	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To view the total number of COMMUNITY attributes found, use the `show ip bgp summary` command. The text line above the route table states the number of COMMUNITY attributes found.

The `show ip bgp community` command without any parameters lists BGP routes with at least one BGP community attribute and the output is the same as for the `show ip bgp` command output.

show ip bgp filter-list

View the routes that match the filter lists.

Syntax `show ip bgp [ipv4 unicast] filter-list as-path-name`

Parameters

ipv4 unicast	(OPTIONAL) Enter the keywords `ipv4 unicast` to view information only related to ipv4 unicast routes.
as-path-name	Enter an AS-PATH access list name. The range is 140 characters.

Command Modes

- EXEC
- EXEC Privilege

Command History	**Version 9.2(0.0)**	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show ip bgp filter-list hello` command shown in the following example.

Field	**Description**
Path source codes	Lists the path sources shown to the right of the last AS number in the Path column: • i = internal route entry • a = aggregate route entry • c = external confederation route entry • n = network route entry • r = redistributed route entry

Field	Description
Next Hop	Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then local routes exist in the routing table.
Metric	Displays the BGP route's metric, if assigned.
LocPrf	Displays the BGP LOCAL_PREF attribute for the route.
Weight	Displays the route's weight.
Path	Lists all the ASs the route passed through to reach the destination network.

Example

```
Dell#show ip bgp filter-list hello
BGP table version is 80227, local router ID is 120.1.1.1
Status codes: s suppressed, d damped, h history, * valid, >
best
Path source: I - internal, a - aggregate, c - confed-external,
r - redistributed, n -
network
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network    Next Hop              Metric LocPrf Weight
Path
* I 6.1.5.0/24 192.100.11.2           20000   9999    0 ?
* I            192.100.8.2            20000   9999    0 ?
* I            192.100.9.2            20000   9999    0 ?
* I            192.100.10.2           20000   9999    0 ?
*>I            6.1.5.1                20000   9999    0 ?
* I            6.1.6.1                20000   9999    0 ?
* I            6.1.20.1               20000   9999    0 ?
* I            6.1.6.0/24 192.100.11.2  20000   9999    0 ?
* I            192.100.8.2            20000   9999    0 ?
* I            192.100.9.2            20000   9999    0 ?
* I            192.100.10.2           20000   9999    0 ?
*>I            6.1.5.1                20000   9999    0 ?
* I            6.1.6.1                20000   9999    0 ?
* I            6.1.20.1               20000   9999    0 ?
* I            6.1.20.0/24 192.100.11.2 20000   9999    0 ?
* I            192.100.8.2            20000   9999    0 ?
* I            192.100.9.2            20000   9999    0 ?
* I            192.100.10.2           20000   9999    0 ?
Dell#
```

show ip bgp flap-statistics

View flap statistics on BGP routes.

Syntax `show ip bgp [ipv4 unicast] flap-statistics [ip-address [mask]] [filter-list as-path-name] [regexp regular-expression]`

Parameters

ipv4 unicast	(OPTIONAL) Enter the keywords `ipv4 unicast` to view information only related to ipv4 unicast routes.

ip-address	(OPTIONAL) Enter the IP address (in dotted decimal format) of the BGP network to view information only on that network.
mask	(OPTIONAL) Enter the network mask (in slash prefix (/x) format) of the BGP network address.
filter-list *as-path-name*	(OPTIONAL) Enter the keyword `filter-list` then the name of a configured AS-PATH ACL. The range is 140 characters.
regexp *regular-expression*	Enter a regular expression then use one or a combination of the following characters to match. The range is 256 characters. • `.` = (period) any single character (including a white space). • `*` = (asterisk) the sequences in a pattern (zero or more sequences). • `+` = (plus) the sequences in a pattern (one or more sequences). • `?` = (question mark) sequences in a pattern (either zero or one sequences). **NOTE:** Enter an escape sequence (CTRL+v) prior to entering the `?` regular expression. • `[ ]` = (brackets) a range of single-character patterns. • `( )` = (parenthesis) groups a series of pattern elements to a single element. • `{ }` = (braces) minimum and the maximum match count. • `^` = (caret) the beginning of the input string. If you use the caret at the beginning of a sequence or range, it matches on everything BUT the characters specified. • `$` = (dollar sign) the end of the output string.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show ip bgp flap` command shown in the following example.

Field	Description
Network	Displays the network ID to which the route is flapping.
From	Displays the IP address of the neighbor advertising the flapping route.

Field	Description
Flaps	Displays the number of times the route flapped.
Duration	Displays the hours:minutes:seconds since the route first flapped.
Reuse	Displays the hours:minutes:seconds until the flapped route is available.
Path	Lists all the ASs the flapping route passed through to reach the destination network.

Example

```
Dell>show ip bgp flap-statistics
BGP table version is 210851, local router ID is 63.114.8.2
Status codes: s suppressed, d damped, h history, * valid, >
best
Path source: I - internal, a - aggregate, c - confed-external,
  r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete

 Network      From      Flaps      Duration      Reuse
Path
Dell>
```

show ip bgp inconsistent-as

View routes with inconsistent originating autonomous system (AS) numbers; that is, prefixes that are announced from the same neighbor AS but with a different AS-Path.

Syntax `show ip bgp [ipv4 unicast] inconsistent-as`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show ip bgp inconsistent-as` command shown in the following example.

Field	Description
Network	Displays the destination network prefix of each BGP route.
Next Hop	Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then local routes exist in the routing table.
Metric	Displays the BGP route’s metric, if assigned.

Field	Description
LocPrf	Displays the BGP LOCAL_PREF attribute for the route.
Weight	Displays the route’s weight.
Path	Lists all the ASs the route passed through to reach the destination network.

Example

```
Dell>show ip bgp inconsistent-as
BGP table version is 280852, local router ID is 10.1.2.100
Status codes: s suppressed, d damped, h history, * valid, >
best
Path source: I - internal, c - confed-external, r -
redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network Next  Hop         Metric LocPrf Weight Path
*  3.0.0.0/8     63.114.8.33                0 18508 209 7018
80 i
*                63.114.8.34                0 18508 209 7018
80 i
*                63.114.8.60                0 18508 209 7018
80 i
*>               63.114.8.33                0 18508 701 80 i
*> 3.18.135.0/24 63.114.8.60                0 18508 209 7018 ?
*                63.114.8.34                0 18508 209 7018 ?
*                63.114.8.33                0 18508 701 7018 ?
*                63.114.8.33                0 18508 209 7018 ?
*> 4.0.0.0/8     63.114.8.60                0 18508 209 1 i
*                63.114.8.34                0 18508 209 1 i
*                63.114.8.33                0 18508 701 1 i
*                63.114.8.33                0 18508 209 1 i
*  6.0.0.0/20    63.114.8.60                0 18508 209 3549 i
*                63.114.8.34                0 18508 209 3549 i
*>               63.114.8.33      0         0 18508 ?
*                63.114.8.33                0 18508 209 3549 i
*  9.2.0.0/16    63.114.8.60                0 18508 209 701 i
*                63.114.8.34                0 18508 209 701 i
--More--
```

show ip bgp neighbors

Allows you to view the information BGP neighbors exchange.

Syntax

`show ip bgp [`*`ipv4 unicast`*`] neighbors [`*`ip-address`*` [advertised-routes | dampened-routes | detail | flap-statistics | routes | {received-routes [`*`network`*` [`*`network-mask`*`]]} | {denied-routes [`*`network`*` [`*`network-mask`*`]]}]`

Parameters

ipv4 unicast	(OPTIONAL) Enter the keywords `ipv4 unicast` to view information only related to ipv4 unicast routes.
ip-address	(OPTIONAL) Enter the IP address of the neighbor to view only BGP information exchanged with that neighbor.

advertised-routes	(OPTIONAL) Enter the keywords `advertised-routes` to view only the routes the neighbor sent.
dampened-routes	(OPTIONAL) Enter the keywords `dampened-routes` to view information on dampened routes from the BGP neighbor.
detail	(OPTIONAL) Enter the keyword `detail` to view neighbor-specific internal information for the IPv4 Unicast address family.
flap-statistics	(OPTIONAL) Enter the keywords `flap-statistics` to view flap statistics on the neighbor's routes.
routes	(OPTIONAL) Enter the keyword `routes` to view only the neighbor's feasible routes.
received-routes [*network* [*network-mask*]	(OPTIONAL) Enter the keywords `received-routes` then either the network address (in dotted decimal format) or the network mask (in slash prefix format) to view all information received from neighbors. **NOTE:** Configure the `neighbor soft-reconfiguration inbound` command prior to viewing all the information received from the neighbors.
denied-routes [*network* [*network-mask*]	(OPTIONAL) Enter the keywords `denied-routes` then either the network address (in dotted decimal format) or the network mask (in slash prefix format) to view all information on routes denied via neighbor inbound filters.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

After a peer reset, the contents of the notification log messages is displayed in hex values for debugging.

The following describes the `show ip bgp neighbors` command shown in the following examples.

The Lines Beginning with:	Description
BGP neighbor	Displays the BGP neighbor address and its AS number. The last phrase in the line indicates whether the link between the BGP router and its neighbor is an external or internal one. If they are located in the same AS, the link is internal; otherwise the link is external.

The Lines Beginning with:	Description
BGP version	Displays the BGP version (always version 4) and the remote router ID.
BGP state	Displays the neighbor's BGP state and the amount of time in hours:minutes:seconds it has been in that state.
Last read	This line displays the following information: • last read is the time (hours:minutes:seconds) the router read a message from its neighbor • hold time is the number of seconds configured between messages from its neighbor • keepalive interval is the number of seconds between keepalive messages to help ensure that the TCP session is still alive.
Received messages	This line displays the number of BGP messages received, the number of notifications (error messages), and the number of messages waiting in a queue for processing.
Sent messages	The line displays the number of BGP messages sent, the number of notifications (error messages), and the number of messages waiting in a queue for processing.
Received updates	This line displays the number of BGP updates received and sent.
Soft reconfiguration	This line indicates that soft reconfiguration inbound is configured.
Minimum time	Displays the minimum time, in seconds, between advertisements.
(list of inbound and outbound policies)	Displays the policy commands configured and the names of the Route map, AS-PATH ACL, or Prefix list configured for the policy.
For address family:	Displays the IPv4 Unicast as the address family.
BGP table version	Displays which version of the primary BGP routing table the router and the neighbor are using.
accepted prefixes	Displays the number of network prefixes the router accepts and the amount of memory used to process those prefixes.
Prefix advertised	Displays the number of network prefixes advertised, the number rejected, and the number withdrawn from the BGP routing table.
Connections established	Displays the number of TCP connections established and dropped between the two peers to exchange BGP information.

The Lines Beginning with:	Description
Last reset	Displays the amount of time since the peering session was last reset. Also states if the peer resets the peering session. If the peering session was never reset, the word never is displayed.
Local host:	Displays the peering address of the local router and the TCP port number.
Foreign host:	Displays the peering address of the neighbor and the TCP port number.

Example (S4810 S4820T)

```
Dell#show ip bgp neighbors
BGP neighbor is 10.10.10.1, remote AS 23456, external link
  BGP version 4, remote router ID 10.10.10.1
  BGP state ESTABLISHED, in this state for 00:00:35
. . .
  Capabilities received from neighbor for IPv4 Unicast :
    MULTIPROTO_EXT(1)
    ROUTE_REFRESH(2)
    4_OCTECT_AS(65)
    ADD_PATH (69)
    CISCO_ROUTE_REFRESH(128)
```

Example

```
Dell#show ip bgp neighbors

BGP neighbor is 100.10.10.2, remote AS 200, external link
  BGP version 4, remote router ID 192.168.2.101
  BGP state ESTABLISHED, in this state for 00:16:12
  Last read 00:00:12, last write 00:00:03
  Hold time is 180, keepalive interval is 60 seconds
Received 1404 messages, 0 in queue
  3 opens, 1 notifications, 1394 updates
  6 keepalives, 0 route refresh requests
 Sent 48 messages, 0 in queue
  3 opens, 2 notifications, 0 updates
  43 keepalives, 0 route refresh requests
Minimum time between advertisement runs is 30 seconds
  Minimum time before advertisements start is 0 seconds

  Capabilities received from neighbor for IPv4 Unicast :
    MULTIPROTO_EXT(1)
    ROUTE_REFRESH(2)
    CISCO_ROUTE_REFRESH(128)

  Capabilities advertised to neighbor for IPv4 Unicast :
    MULTIPROTO_EXT(1)
    ROUTE_REFRESH(2)
    ROUTE_REFRESH(2)
    GRACEFUL_RESTART(64)
    CISCO_ROUTE_REFRESH(128)

  Route map for incoming advertisements is test
  Maximum prefix set to 4 with threshold 75

  For address family: IPv4 Unicast
  BGP table version 34, neighbor version 34
  5 accepted prefixes consume 20 bytes
  Prefix advertised 0, denied 4, withdrawn 0

Prefixes accepted 1 (consume 4 bytes), withdrawn 0 by peer
  Prefixes advertised 0, rejected 0, withdrawn 0 from peer

  Connections established 2; dropped 1
  Last reset 00:18:21, due to Maximum prefix limit reached
```

Example (Advertised-Routes)

```
Dell>show ip bgp neighbors 192.14.1.5 advertised-routes

BGP table version is 74103, local router ID is 33.33.33.33
Status codes: s suppressed, S stale, d damped, h history, *
valid, > best
Path source: I - internal, a - aggregate, c - confed-external,
r - redistributed,
n - network
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network Next     Hop            Metric LocPrf  Weight Path
*>r 1.10.1.0/24     0.0.0.0         5000             32768 ?
*>r 1.11.0.0/16     0.0.0.0         5000             32768 ?
.....
...
*>I 223.94.249.0/24 223.100.4.249   0        100         0 ?
*>I 223.94.250.0/24 223.100.4.250   0        100         0 ?
*>I 223.100.0.0/16  223.100.255.254 0        100         0 ?
Total number of prefixes: 74102
```

Example (Received-Routes)

```
BGP table version is 13, local router ID is 120.10.10.1
Status codes: s suppressed, S stale, d damped, h history, *
valid, > best
Path source: I - internal, a - aggregate, c - confed-external,
r - redistributed
n - network, D - denied, S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network       Next Hop     Metric LocPrf   Weight Path
D   70.70.21.0/24 100.10.10.2           0   0 100 200 ?
D   70.70.22.0/24 100.10.10.2           0   0 100 200 ?
D   70.70.23.0/24 100.10.10.2           0   0 100 200 ?
D   70.70.24.0/24 100.10.10.2           0   0 100 200 ?
*>  70.70.25.0/24 100.10.10.2           0   0 100 200 ?
*>  70.70.26.0/24 100.10.10.2    0      0   0 100 200 ?
*>  70.70.27.0/24 100.10.10.2    0      0   0 100 200 ?
*>  70.70.28.0/24 100.10.10.2    0      0   0 100 200 ?
*>  70.70.29.0/24 100.10.10.2    0      0   0 100 200 ?
Dell#
```

Example (denied-routes)

```
Dell#show ip bgp neighbors 100.10.10.2 denied-routes
4 denied paths using 205 bytes of memory
BGP table version is 34, local router ID is 100.10.10.2
Status codes: s suppressed, S stale, d damped, h history, *
valid, > best
Path source: I - internal, a - aggregate, c - confed-external,
r - redistributed
n - network, D - denied, S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network        Next Hop     Metric LocPrf Weight Path
D  70.70.21.0/24  100.10.10.2           0    0 100 200 ?
D  70.70.22.0/24  100.10.10.2           0    0 100 200 ?
```

```
D  70.70.23.0/24  100.10.10.2            0    0 100 200 ?
D  70.70.24.0/24  100.10.10.2            0    0 100 200 ?
Dell#
```

Related Commands

show ip bgp — views the current BGP routing table.

show ip bgp next-hop

View all next hops (using learned routes only) with current reachability and flap status. This command only displays one path, even if the next hop is reachable by multiple paths.

Syntax

`show ip bgp next-hop`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show ip bgp next-hop` command shown in the following example.

Field	Description
Next-hop	Displays the next-hop IP address.
Via	Displays the IP address and interface used to reach the next hop.
RefCount	Displays the number of BGP routes using this next hop.
Cost	Displays the cost associated with using this next hop.
Flaps	Displays the number of times the next hop has flapped.
Time Elapsed	Displays the time elapsed since the next hop was learned. If the route is down, this field displays time elapsed since the route went down.

Example

```
Dell>show ip bgp next-hop
  Next-hop    Via                   RefCount Cost Flaps Time
Elapsed
  63.114.8.33 63.114.8.33, Gi 12/22   240984   0     0 00:18:25
  63.114.8.34 63.114.8.34, Gi 12/22   135152   0     0 00:18:13
  63.114.8.35 63.114.8.35, Gi 12/22        1   0     0 00:18:07
  63.114.8.60 63.114.8.60, Gi 12/22   135155   0     0 00:18:11
Dell>
```

show ip bgp paths

View all the BGP path attributes in the BGP database.

Syntax `show ip bgp paths [regexp regular-expression]`

Parameters

regexp *regular-expression*	Enter a regular expression then use one or a combination of the following characters to match: • `.` = (period) any single character (including a white space). • `*` = (asterisk) the sequences in a pattern (zero or more sequences). • `+` = (plus) the sequences in a pattern (one or more sequences). • `?` = (question mark) sequences in a pattern (either zero or one sequences). **NOTE:** Enter an escape sequence (CTRL+v) prior to entering the `?` regular expression. • `[ ]` = (brackets) a range of single-character patterns. • `( )` = (parenthesis) groups a series of pattern elements to a single element. • `{ }` = (braces) minimum and the maximum match count. • `^` = (caret) the beginning of the input string. If you use the caret at the beginning of a sequence or range, it matches on everything BUT the characters specified. • `$` = (dollar sign) the end of the output string.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show ip bgp path` command shown in the following example.

Field	Description
Total	Displays the total number of BGP path attributes.
Address	Displays the internal address where the path attribute is stored.
Hash	Displays the hash bucket where the path attribute is stored.
Refcount	Displays the number of BGP routes using this path attribute.
Metric	Displays the MED attribute for this path attribute.

Field	Description
Path	Displays the AS path for the route, with the origin code for the route listed last. Numbers listed between braces {} are AS_SET information.

Example

```
Dell#show ip bgp path
Total 16 Paths
Address      Hash Refcount   Metric Path
0x1efe7e5c   15       10000          32 ?
0x1efe7e1c   71       10000          23 ?
0x1efe7ddc   127      10000          22 ?
0x1efe7d9c   183      10000          43 ?
0x1efe7d5c   239      10000          42 ?
0x1efe7c9c   283          6          {102 103} ?
0x1efe7b1c   287        336 20000    ?
0x1efe7d1c   295      10000          13 ?
0x1efe7c5c   339          6          {92 93} ?
0x1efe7cdc   351      10000          12 ?
0x1efe7c1c   395          6          {82 83} ?
0x1efe7bdc   451          6          {72 73} ?
0x1efe7b5c   491         78       0  ?
0x1efe7adc   883          2     120  i
0x1efe7e9c   983      10000          33 ?
0x1efe7b9c   1003         6       0  i
Dell#
```

show ip bgp paths as-path

View all unique AS-PATHs in the BGP database.

Syntax `show ip bgp paths as-path`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show ip bgp paths as-path` command shown in the following example.

Field	Description
Address	Displays the internal address where the path attribute is stored.
Hash	Displays the hash bucket where the path attribute is stored.
Refcount	Displays the number of BGP routes using these AS-Paths.

Field	Description
AS-Path	Displays the AS paths for this route, with the origin code for the route listed last. Numbers listed between braces {} are AS_SET information.

Example

```
Dell#show ip bgp paths as-path
Total 13 AS-Paths
Address      Hash Refcount AS-Path
0x1ea3c1ec   251         1   42
0x1ea3c25c   251         1   22
0x1ea3c1b4   507         1   13
0x1ea3c304   507         1   33
0x1ea3c10c   763         1   {92 93}
0x1ea3c144   763         1   {102 103}
0x1ea3c17c   763         1   12
0x1ea3c2cc   763         1   32
0x1ea3c09c   764         1   {72 73}
0x1ea3c0d4   764         1   {82 83}
0x1ea3c224   1019        1   43
0x1ea3c294   1019        1   23
0x1ea3c02c   1021        4
Dell#
```

show ip bgp paths community

View all unique COMMUNITY numbers in the BGP database.

Syntax `show ip bgp paths community`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show ip bgp paths community` command shown in the following example.

Field	Description
Address	Displays the internal address where the path attribute is stored.
Hash	Displays the hash bucket where the path attribute is stored.
Refcount	Displays the number of BGP routes using these communities.
Community	Displays the community attributes in this BGP path.

Example

```
E1200-BGP>show ip bgp paths community
Total 293 Communities
Address      Hash   Refcount Community
0x1ec88a5c      3          4 209:209 209:6059 209:31272
3908:900 19092:300
0x1e0f10ec     15          4 209:209 209:3039 209:31272
3908:900 19092:300
0x1c902234     37          2 209:209 209:7193 209:21362
3908:900 19092:300
0x1f588cd4     41         24 209:209 209:6253 209:21362
3908:900 19092:300
0x1e805884     46          2 209:209 209:21226 286:777
286:3033 1899:3033
64675:21092
0x1e433f4c     46          8 209:209 209:5097 209:21362
3908:900 19092:300
0x1f173294     48         16 209:209 209:21226 286:40 286:777
286:3040 5606:40
12955:5606
0x1c9f8e24     50          6 209:209 209:4069 209:21362
3908:900 19092:300
0x1c9f88e4     53          4 209:209 209:3193 209:21362
3908:900 19092:300
0x1f58a944     57          6 209:209 209:2073 209:21362
3908:900 19092:300
0x1ce6be44     80          2 209:209 209:999 209:40832
0x1c6e2374     80          2 209:777 209:41528
0x1f58ad6c     82         46 209:209 209:41528
0x1c6e2064     83          2 209:777 209:40832
0x1f588ecc     85        570 209:209 209:40832
0x1f57cc0c     98          2 209:209 209:21226 286:3031
13646:1044 13646:1124
13646:1154 13646:1164 13646:1184 13646:1194 13646:1204
13646:1214 13646:1224
13646:1234 13646:1244 13646:1254 13646:1264 13646:3000
0x1d65b2ac     117         6 209:209 209:999 209:31272
0x1f5854ac     119        18 209:209 209:21226 286:108 286:111
286:777 286:3033
517:5104
```

show ip bgp peer-group

Allows you to view information on the BGP peers in a peer group.

Syntax

`show ip bgp [`*`ipv4 unicast`*`] peer-group [`*`peer-group-name`*` [detail | summary]]`

Parameters

ipv4 unicast	(OPTIONAL) Enter the keywords `ipv4 unicast` to view information only related to ipv4 unicast routes.
peer-group-name	(OPTIONAL) Enter the name of a peer group to view information about that peer group only.
detail	(OPTIONAL) Enter the keyword `detail` to view detailed status information of the peers in that peer group.

summary	(OPTIONAL) Enter the keyword `summary` to view status information of the peers in that peer group. The output is the same as that found in the `show ip bgp summary` command.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show ip bgp peer-group` command shown in the following example.

Line beginning with:	Description
Peer-group	Displays the peer group's name.
Administratively shut	Displays the peer group's status if the peer group is not enabled. If you enable the peer group, this line is not displayed.
BGP version	Displays the BGP version supported.
Minimum time	Displays the time interval between BGP advertisements.
For address family	Displays IPv4 Unicast as the address family.
BGP neighbor	Displays the name of the BGP neighbor.
Number of peers	Displays the number of peers currently configured for this peer group.
Peer-group members:	Lists the IP addresses of the peers in the peer group. If the address is outbound optimized, an * is displayed next to the IP address.

Example (S4810 S4820T)

```
Dell#show ip bgp peer-group

Peer-group pg1
  BGP version 4
  Minimum time between advertisement runs is 30 seconds

  For address family: IPv4 Unicast
  BGP neighbor is pg1
Number of peers in this group 4
  Update packing has 4_OCTECT_AS support enabled
  Add-path support enabled
  Peer-group members (* - outbound optimized):
     1.1.1.5
     1.1.1.6
     10.10.10.2*
     20.20.20.100
```

Example

```
Dell#show ip bgp peer-group

Peer-group RT-PEERS
Description: ***peering-with-RT***
BGP version 4
Minimum time between advertisement runs is 30 seconds

For address family: IPv4 Unicast
BGP neighbor is RT-PEERS
Number of peers in this group 20
Peer-group members (* - outbound optimized):
  12.1.1.2*
  12.1.1.3*
  12.1.1.4*
  12.1.1.5*
  12.1.1.6*
  12.2.1.2*
  12.2.1.3*
  12.2.1.4*
  12.2.1.5*
  12.2.1.6*
  12.3.1.2*
  12.3.1.3*
  12.3.1.4*
  12.3.1.5*
  12.3.1.6*
  12.4.1.2*
  12.4.1.3*
  12.4.1.4*
  12.4.1.5*
  12.4.1.6*
```

Related Commands

neighbor peer-group (assigning peers) — assigns a peer to a peer-group.

neighbor peer-group (creating group) — creates a peer group.

show ip bgp regexp

Display the subset of the BGP routing table matching the regular expressions specified.

Syntax `show ip bgp regexp` *`regular-expression`* `[`*`character`*`]`

Parameters

regular-expression [*character*]	Enter a regular expression then use one or a combination of the following characters to match: • `.` = (period) any single character (including a white space). • `*` = (asterisk) the sequences in a pattern (zero or more sequences). • `+` = (plus) the sequences in a pattern (one or more sequences). • `?` = (question mark) sequences in a pattern (either zero or one sequences).

NOTE: Enter an escape sequence (CTRL+v) prior to entering the `?` regular expression.

- `[ ]` = (brackets) a range of single-character patterns.
- `( )` = (parenthesis) groups a series of pattern elements to a single element.
- `{ }` = (braces) minimum and the maximum match count.
- `^` = (caret) the beginning of the input string. If you use the caret at the beginning of a sequence or range, it matches on everything BUT the characters specified.
- `$` = (dollar sign) the end of the output string.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show ip bgp regexp` command shown in the following example.

Field	Description
Network	Displays the destination network prefix of each BGP route.
Next Hop	Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then non-BGP routes exist in the router's routing table.
Metric	Displays the BGP router's metric, if assigned.
LocPrf	Displays the BGP LOCAL_PREF attribute for the route.
Weight	Displays the route's weight
Path	Lists all the AS paths the route passed through to reach the destination network.

Example (S4810)

```
Dell#show ip bgp regexp ^2914+
BGP table version is 3700481, local router ID is 63.114.8.35
Status codes: s suppressed, S stale, d damped, h history, *
valid, > best
Path source: I - internal, a - aggregate, c - confed-external,
r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete
    Network        Next Hop   Metric LocPrf Weight Path
*>I 3.0.0.0/8      1.1.1.2         0 100         0 2914 1239 80
i
*>I 4.0.0.0/8      1.1.1.2         0 100         0 2914 3356 i
*>I 4.17.225.0/24 1.1.1.2         0 100         0 2914 11853
11853 11853 11853 11853 6496
*>I 4.17.226.0/23 1.1.1.2         0 100         0 2914 11853
11853 11853 11853 11853 6496
*>I 4.17.251.0/24 1.1.1.2         0 100         0 2914 11853
11853 11853 11853 11853 6496
*>I 4.17.252.0/23 1.1.1.2         0 100         0 2914 11853
```

```
11853 11853 11853 11853 6496
*>I 4.19.2.0/23   1.1.1.2        0 100         0 2914 701
6167 6167 6167 i
*>I 4.19.16.0/23  1.1.1.2        0 100         0 2914 701
6167 6167 6167 i
*>I 4.21.80.0/22  1.1.1.2        0 100         0 2914 174
4200 16559 i
*>I 4.21.82.0/24  1.1.1.2        0 100         0 2914 174
4200 16559 i
*>I 4.21.252.0/23 1.1.1.2        0 100         0 2914 701
6389 8063 19198 i
*>I 4.23.180.0/24 1.1.1.2        0 100         0 2914 3561
6128 30576 i
*>I 4.36.200.0/21 1.1.1.2        0 100         0 2914 14742
11854 14135 i
*>I 4.67.64.0/22  1.1.1.2        0 100         0 2914 11608
19281 i
*>I 4.78.32.0/21  1.1.1.2        0 100         0 2914 3491
29748 i
*>I 6.1.0.0/16    1.1.1.2        0 100         0 2914 701 668
i
*>I 6.2.0.0/22    1.1.1.2        0 100         0 2914 701 668
i
*>I 6.3.0.0/18    1.1.1.2        0 100         0 2914 701 668
i
```

show ip bgp summary

Allows you to view the status of all BGP connections.

Syntax `show ip bgp [ipv4 unicast] summary`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show ip bgp summary` command shown in the following example.

Field	Description
BGP router identifier	Displays the local router ID and the AS number.
BGP table version	Displays the BGP table version and the main routing table version.
network entries	Displays the number of network entries, route paths, and the amount of memory used to process those entries.

Field	Description
paths	Displays the number of paths and the amount of memory used.
denied paths	Displays the number of denied paths and the amount of memory used.
BGP path attribute entries	Displays the number of BGP path attributes and the amount of memory used to process them.
BGP AS-PATH entries	Displays the number of BGP AS_PATH attributes processed and the amount of memory used to process them.
BGP community entries	Displays the number of BGP COMMUNITY attributes processed and the amount of memory used to process them. The `show ip bgp community` command provides more details on the COMMUNITY attributes.
Dampening enabled	Displayed only when you enable dampening. Displays the number of paths designated as history, dampened, or penalized.
Neighbor	Displays the BGP neighbor address.
AS	Displays the AS number of the neighbor.
MsgRcvd	Displays the number of BGP messages that neighbor received.
MsgSent	Displays the number of BGP messages that neighbor sent.
TblVer	Displays the version of the BGP table that was sent to that neighbor.
InQ	Displays the number of messages from that neighbor waiting to be processed.
OutQ	Displays the number of messages waiting to be sent to that neighbor. If a number appears in parentheses, the number represents the number of messages waiting to be sent to the peer group.
Up/Down	Displays the amount of time that the neighbor is in the Established stage. If the neighbor has never moved into the Established stage, the word never is displayed. The output format is:

Time Established	Display Example
< 1 day	00:12:23 (hours:minutes:seconds)
< 1 week	1d21h (DaysHours)
> 1 week	11w2d (WeeksDays)

Field	Description
State/Pfxrcd	If the neighbor is in Established stage, the number of network prefixes received. If a maximum limit was configured with the `neighbor maximum-prefix` command, (prfxd) appears in this column. If the neighbor is not in Established stage, the current stage is displayed (Idle, Connect, Active, OpenSent, OpenConfirm). When the peer is transitioning between states and clearing the routes received, the phrase (Purging) may appear in this column. If the neighbor is disabled, the phrase (Admin shut) appears in this column.

Example (S4810)

```
Dell#show ip bgp summary
BGP router identifier 120.10.10.1, local AS number 100
BGP table version is 34, main routing table version 34
9 network entrie(s) using 1372 bytes of memory
5 paths using 380 bytes of memory
4 denied paths using 164 bytes of memory
BGP-RIB over all using 385 bytes of memory
2 BGP path attribute entrie(s) using 168 bytes of memory
1 BGP AS-PATH entrie(s) using 39 bytes of memory
1 BGP community entrie(s) using 43 bytes of memory
2 neighbor(s) using 7232 bytes of memory

Neighbor   AS  MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/
Pfx
100.10.10.2 200     46     41     34   0    0 00:14:33    5
120.10.10.2 300     40     47     34   0    0 00:37:10    0
Dell#
```

show running-config bgp

To display the current BGP configuration, use this feature.

Syntax `show running-config bgp`

Defaults none

Command Modes EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

timers bgp

Adjust the BGP Keep Alive and Hold Time timers.

Syntax	`timers bgp` *`keepalive holdtime`* To return to the default, use the `no timers bgp` command.
Parameters	
	keepalive — Enter a number for the time interval, in seconds, between keepalive messages sent to the neighbor routers. The range is from 1 to 65535. The default is **60 seconds**.
	holdtime — Enter a number for the time interval, in seconds, between the last keepalive message and declaring the router dead. The range is from 3 to 65535. The default is **180 seconds**.
Defaults	none
Command Modes	EXEC Privilege
Command History	Version 9.2(0.0) — Introduced on the MXL 10/40GbE Switch IO Module.

MBGP Commands

Multiprotocol BGP (MBGP) is an enhanced BGP that enables multicast routing policy throughout the internet and connecting multicast topologies between BGP and autonomous systems (ASs).

MBGP is implemented as per IETF RFC 1858.

debug ip bgp dampening

View information on routes being dampened.

Syntax	`debug ip bgp ipv4 multicast dampening` To disable debugging, use the `no debug ip bgp ipv4 multicast dampening` command.
Parameters	
	dampening — Enter the keyword `dampening` to clear route flap dampening information.
Command Modes	EXEC Privilege

Command History	Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

distance bgp

Define an administrative distance for routes.

Syntax

`distance bgp` *`external-distance internal-distance local-distance`*

To return to default values, use the `no distance bgp` command.

Parameters

external-distance	Enter a number to assign to routes learned from a neighbor external to the AS. The range is from 1 to 255. The default is **20**.
internal-distance	Enter a number to assign to routes learned from a router within the AS. The range is from 1 to 255. The default is **200**.
local-distance	Enter a number to assign to routes learned from networks listed in the network command. The range is from 1 to 255. The default is **200**.

Defaults

- external-distance = **20**
- internal-distance = **200**
- local-distance = **200**

Command Modes

ROUTER BGP (conf-router_bgp_af)

Command History	Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

CAUTION: Dell Networking OS recommends that you do not change the administrative distance of internal routes. Changing the administrative distances may cause routing table inconsistencies.

The higher the administrative distance assigned to a route means that your confidence in that route is low. Routes assigned an administrative distance of 255 are not installed in the routing table. Routes from confederations are treated as internal BGP routes.

show ip bgp dampened-paths

View BGP routes that are dampened (non-active).

Syntax

`show ip bgp [ipv4 unicast] dampened-paths`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show ip bgp damp` command shown in the following example.

Field	Description
Network	Displays the network ID to which the route is dampened.
From	Displays the IP address of the neighbor advertising the dampened route.
Reuse	Displays the hour:minutes:seconds until the dampened route is available.
Path	Lists all the ASs the dampened route passed through to reach the destination network.

Example

```
Dell>show ip bgp dampened-paths
BGP table version is 210708, local router ID is 63.114.8.2
Status codes: s suppressed, d damped, h history, * valid, >
best
Path source: I - internal, a - aggregate, c - confed-external,
r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network      From       Reuse       Path
Dell>
```

BGP Extended Communities (RFC 4360)

BGP Extended Communities, as defined in RFC 4360, is an optional transitive BGP attribute.

BGP Extended Communities provides two major advantages over Standard Communities:

- The range is extended from 4-octet (AA:NN) to 8-octet (Type:Value) to provide enough number communities.
- Communities are structured using a new “Type” field (1 or 2-octets), allowing you to provide granular control/filter routing information based on the type of extended communities.

set extcommunity rt

To set Route Origin community attributes in Route Map, use this feature.

Syntax	`set extcommunity rt {as4 ASN4:NN [non-trans] | ASN:NNNN [non-trans] | IPADDR:NN [non-trans]} [additive]` To delete the Route Origin community, use the `no set extcommunity` command.

Parameters

as4 *ASN4:NN*	Enter the keyword `as4` then the 4-octet AS specific extended community number in the format ASN4:NN (4-byte AS number:2-byte community value).
ASN:NNNN	Enter the 2-octet AS specific extended community number in the format ASN:NNNN (2-byte AS number:4-byte community value).
IPADDR:NN	Enter the IP address specific extended community in the format IPADDR:NN (4-byte IPv4 Unicast Address:2-byte community value).
additive	(OPTIONAL) Enter the keyword `additive` to add to the existing extended community.
non-trans	(OPTIONAL) Enter the keywords `non-trans` to indicate a non-transitive BGP extended community.

Defaults	none
Command Modes	ROUTE MAP (config-route-map)

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

If the set community `rt` and `soo` are in the same route-map entry, the behavior defines as:

- If the `rt` option comes before `soo`, with or without the `additive` option, `soo` overrides the communities `rt` sets.
- If the `rt` option comes after `soo`, without the `additive` option, `rt` overrides the communities `soo` sets.
- If the `rt` with the `additive` option comes after `soo`, `rt` adds the communities `soo` sets.

Related Commands

set extcommunity soo — sets the extended community site-of-origin in the route-map.

set extcommunity soo

To set extended community site-of-origin in Route Map, use this feature.

Syntax	`set extcommunity soo {as4 ASN4:NN | ASN:NNNN | IPADDR:NN [non-trans]}` To delete the site-of-origin community, use the `no set extcommunity` command.

Parameters

as4 *ASN4:NN*	Enter the keyword `as4` then the 4-octet AS specific extended community number in the format ASN4:NN (4-byte AS number:2-byte community value).
ASN:NNNN	Enter the 2-octet AS specific extended community number in the format ASN:NNNN (2-byte AS number:4-byte community value).
IPADDR:NN	Enter the IP address specific extended community in the format IPADDR:NN (4-byte IPv4 Unicast Address:2-byte community value).
non-trans	(OPTIONAL) Enter the keywords `non-trans` to indicate a non-transitive BGP extended community.

Defaults	none
Command Modes	ROUTE MAP (config-route-map)

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

If the set community `rt` and `soo` are in the same route-map entry, the behavior defines as:

- If the `rt` option comes before `soo`, with or without the `additive` option, `soo` overrides the communities `rt` sets.
- If the `rt` option comes after `soo`, without the `additive` option, `rt` overrides the communities `soo` sets.
- If the `rt` with the `additive` option comes after `soo`, `rt` adds the communities `soo` sets.

Related Commands

set extcommunity rt — sets the extended community route origins using the route-map.

show ip bgp paths extcommunity

To display all BGP paths having extended community attributes, use this feature.

Syntax `show ip bgp paths extcommunity`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show ip bgp paths extcommunity` command shown in the following example.

Field	Description
Address	Displays the internal address where the path attribute is stored.
Hash	Displays the hash bucket where the path attribute is stored.
Refcount	Displays the number of BGP routes using these extended communities.
Community	Displays the extended community attributes in this BGP path.

Example

```
Dell#show ip bgp paths extcommunity
Total 1 Extended Communities

Address     Hash  Refcount Extended Community
0x41d57024  12272 1        RT:7:200 SoO:5:300 SoO:0.0.0.3:1285

Dell#
```

show ip bgp extcommunity-list

View information on all routes with Extended Community attributes.

Syntax `show ip bgp [ipv4 unicast] extcommunity-list [list name]`

Parameters

ipv4 unicast	(OPTIONAL) Enter the keywords `ipv4 unicast` to view information only related to ipv4 unicast routes.
list name	Enter the extended community list name you wish to view. The range is 140 characters.

Command Modes

- EXEC

- EXEC Privilege

Command History	**Version 9.2(0.0)**	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To view the total number of COMMUNITY attributes found, use the `show ip bgp summary` command. The text line above the route table states the number of COMMUNITY attributes found.

The `show ip bgp community` command without any parameters lists BGP routes with at least one BGP community attribute and the output is the same as for the `show ip bgp` command output.

IPv6 BGP Commands

IPv6 Border Gateway Protocol (IPv6 BGP) is supported on the MXL 10/40GbE Switch IO Module.

Border gateway protocol (BGP) is an external gateway protocol that transmits interdomain routing information within and between autonomous systems (AS). BGP version 4 (BGPv4) supports classless interdomain routing and the aggregation of routes and AS paths. Basically, two routers (called neighbors or peers) exchange information including full routing tables and periodically send messages to update those routing tables.

bgp soft-reconfig-backup

To avoid the peer from resending messages, use this command *only* when route-refresh is *not* negotiated.

Syntax

`bgp soft-reconfig-backup`

To return to the default setting, use the `no bgp soft-reconfig-backup` command.

Defaults

Disabled

Command Modes

ROUTER BGP

Command History	**Version 9.2(0.0)**	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

When you enable soft-reconfiguration for a neighbor and you execute the `clear ip bgp soft in` command, the update database stored in the router is replayed and updates are re-evaluated. With this command, the replay and update process is triggered only if route-refresh request is not negotiated with the peer. If the request is indeed negotiated (after executing the `clear ip bgp soft in` command), BGP sends a route-refresh request to the neighbor and receives all of the peer's updates.

Related Commands	clear ip bgp — activates inbound policies without resetting the BGP TCP session.

clear ip bgp ipv6 unicast soft

Clear and reapply policies for IPv6 unicast routes without resetting the TCP connection; that is, perform BGP soft reconfiguration.

Syntax

```
clear ip bgp {* | as-number | ipv4-neighbor-addr | ipv6-
neighbor-addr | peer-group name} ipv6 unicast soft [in | out]
```

Parameters

*	Clear and reapply an asterisk (*) for all BGP sessions.
as-number	Clear and reapply policies for all neighbors belonging to the AS. The range is from 0 to 65535 (2 Byte), from 1 to 4294967295 (4 Byte), or from 0.1 to 0.65535.65535 (Dotted format).
ipv4-neighbor-addr | ipv6-neighbor-addr	Clear and reapply policies for a neighbor.
peer-group name	Clear and reapply policies for all BGP routers in the specified peer group.
ipv6 unicast soft	Clear and reapply policies for all IPv6 unicast routes.
in	Reapply only inbound policies. NOTE: If you enter `soft`, without an `in` or `out` option, both inbound and outbound policies are reset.
out	Reapply only outbound policies. NOTE: If you enter `soft`, without an `in` or `out` option, both inbound and outbound policies are reset.

Command Modes: EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

debug ip bgp ipv6 unicast soft-reconfiguration

Enable soft-reconfiguration debugging for IPv6 unicast routes.

Syntax

`debug ip bgp [`*`ipv4-address`*` | `*`ipv6-address`*` | `*`peer-group-name`*`] ipv6 unicast soft-reconfiguration`

To disable debugging, use the `no debug ip bgp [`*`ipv4-address`*` | `*`ipv6-address`*` | `*`peer-group-name`*`] ipv6 unicast soft-reconfiguration` command.

Parameters

ipv4-address | *ipv6-address*	Enter the IP address of the neighbor on which you want to enable soft-reconfiguration debugging.
peer-group-name	Enter the name of the peer group on which you want to enable soft-reconfiguration debugging.
ipv6 unicast	Debug soft reconfiguration for IPv6 unicast routes.

Defaults Disabled.

Command Modes EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information This command turns on BGP soft-reconfiguration inbound debugging for IPv6 unicast routes. If no neighbor is specified, debug is turned on for all neighbors.

ipv6 prefix-list

Configure an IPv6 prefix list.

Syntax

`ipv6 prefix-list `*`prefix-list name`*

Parameters

prefix-list name	Enter the name of the prefix list. **NOTE:** There is a 140-character limit for prefix list names.

Defaults none

Command Modes CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands show ipv6 prefix-list — View the selected IPv6 prefix-list.

show ipv6 prefix-list

Displays the specified IPv6 prefix list.

Syntax

```
show ipv6 prefix-list detail {prefix-list name} | summary
```

Parameters

detail	Display a detailed description of the selected IPv6 prefix list.
prefix-list name	Enter the name of the prefix list. NOTE: There is a 140-character limit for prefix list names.
summary	Display a summary of RPF routes.

Command Modes EXEC

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands ipv6 prefix-list — configures an IPv6 prefix-list.

IPv6 MBGP Commands

Multiprotocol BGP (MBGP) is an enhanced BGP that enables multicast routing policy throughout the Internet and connecting multicast topologies between BGP and autonomous systems (AS).

MBGP is implemented as per IETF RFC 1858.

show ipv6 mbgproutes

Display the selected IPv6 MBGP route or a summary of all MBGP routes in the table.

Syntax

```
show ipv6 mbgproutes ipv6-address prefix-length | summary
```

Parameters

ipv6-address prefix-length	(OPTIONAL) Enter the IPv6 address in the x:x:x:x::x format then the prefix length in the /x format. The range is from /0 to /128. NOTE: The :: notation specifies successive hexadecimal fields of zeros.

	summary	Display a summary of RPF routes.
Command Modes	EXEC	
Command History	**Version 9.2(0.0)**	Introduced on the MXL 10/40GbE Switch IO Module.

10

Content Addressable Memory (CAM)

Content addressable memory (CAM) commands are supported on the Dell Networking MXL 10/40GbE Switch IO Module.

⚠ **WARNING: If you are using these features for the first time, contact Dell Networking Technical Assistance Center (TAC) for guidance.**

CAM Profile Commands

The CAM profiling feature allows you to partition the CAM to best suit your application. For example:

- Configure more Layer 2 forwarding information base (FIB) entries when the system is deployed as a switch.
- Configure more Layer 3 FIB entries when the system is deployed as a router.
- Configure more access control lists (ACLs).
- Optimize the virtual local area network (VLAN) ACL Group feature, which permits group VLANs for IP egress ACLs.

Important Points to Remember

- The Dell Networking Operating System (OS) versions 7.8.1.0 and later support CAM allocations on the MXL 10/40GbE Switch IO Module.
- The CAM configuration is applied to the entire system when you use the CONFIGURATION mode commands. Save the running-configuration to affect the change.
- When budgeting your CAM allocations for ACLs and quality of service (QoS) configurations, remember that ACL and QoS rules might consume more than one CAM entry depending on complexity. For example, transmission control protocol (TCP) and user datagram protocol (UDP) rules with `port range` options might require more than one CAM entry.
- After you install a secondary RPM, copy the running-configuration to the startup-configuration so that the new RPM has the correct CAM profile.
- You MUST save your changes and reboot the system for CAM profiling or allocations to take effect.

cam-acl (Configuration)

Select the default CAM allocation settings or reconfigure a new CAM allocation for Layer 2, IPv4, and IPv6 ACLs, Layer 2 and Layer 3 (IPv4) QoS, Layer 2 Protocol Tunneling (L2PT), IP and MAC source address validation for DHCP, Ethernet Connectivity Fault Management (CFM) ACLs, and Policy-based Routing (PBR).

Syntax

```
cam-acl {default | l2acl number ipv4acl number ipv6acl number
ipv4qos number l2qos number l2pt number ipmacacl number [vman-
qos | vman-qos—dual— number | vman-qos—dual—fp number] ipv4pbr
number} ecfmacl number fcoeacl number iscsioptacl number}
```

Parameters

default	Use the default CAM profile settings and set the CAM as follows: - L3 ACL (ipv4acl): 4 - L2 ACL(l2acl): 5 - IPv6 L3 ACL (ipv6acl): 0 - L3 QoS (ipv4qos): 1 - L2 QoS (l2qos): 1 - L2PT (L2PT): 0 - MAC ACL (IpMacAcl): 0 - VmanDualQos: 0 - EcfmAcl: 0 - FcoeAcl: 4 - iscsiOptAcl: 2
l2acl *number*	Enter the keyword `l2acl` and then the number of l2acl blocks. The range is from 1 to 8.
ipv4acl *number*	Enter the keyword `ipv4acl` and then the number of FP blocks for IPv4. The range is from 0 to 8.
ipv6acl *number*	Enter the keyword `ipv6acl` and then the number of FP blocks for IPv6. The range is from 0 to 4.
ipv4qos *number*	Enter the keyword `ipv4qos` and then the number of FP blocks for IPv4. The range is from 0 to 8.
l2qos *number*	Enter the keyword `l2qos` and then the number of FP blocks for l2 qos. The range is from 1to 8.
l2pt *number*	Enter the keyword `l2pt` and then the number of FP blocks for l2 protocol tunnelling. The range is from 0 to 1.
Ipmacacl *number*	Enter the keyword `ipmacacl` and then the number of FP blocks for IP and MAC ACL. The range is from 0 to 6.
ecfmacl *number*	Enter the keyword `ecfmacacl` and then the number of FP blocks for ECFM ACL. The range is from 0 to 5.
Vman-qos| vman-dual-qos *number*	Enter the keyword `evman-qos` and then the number of FP blocks for VMAN QoS. The range is from 0 to 6.
vman-dual-qos *number*	Enter the keyword `vman-dual-qos` and then the number of FP blocks for VMAN dual QoS. The range is from 0 to 4.
Ipv4pbr *number*	Enter the keyword `ipv4pbr` and then the number of FP blocks for ipv4pbr ACL. The range is from 0 to 8.
Openflow *number*	Enter the keyword `openflow` and then the number of FP blocks for open flow (multiples of 4). The range is from 0 to 8.

fcoeacl *number*	Enter the keyword `fcoeacl` and then the number of FP blocks for FCOE ACL. The range is from 0 to 6.
Iscsioptacl *number*	Enter the keyword `iscsioptacl` and then the number of FP blocks for iSCSI optimization ACL. The range is from 0 to 2.
vrfv4acl *number*	Enter the keyword `vrfv4acl` and then the number of FP blocks for VRF IPv4 ACL. The range is from 0 to 2. NOTE: Use this attribute to specify the number of VRF ACL groups. The total number of VRF ACL groups should not exceed 13. You can assign only one VRF ACL group with an odd numbered value.
l2acl *number* ipv4acl *number* ipv6acl *number*, ipv4qos *number* l2qos *number*, l2pt *number* ipmacacl *number* ecfmacl *number* [vman-qos | vman--qos-dual *number* | vman-qos-dual-fp *number*] ipv4pbr *number*	Allocate space to each CAM region. Enter the CAM profile name then the amount of CAM space to be allotted. The total space allocated must equal 13. The range for ipv4acl is from 1 to 4. The ipv6acl range must be a factor of 2. The total space allocated must equal 13. The range for `ipv4acl` is 1 to 4. The `ipv6acl` range must be a factor of 2. The `vman-qos-dual-fp` *`number`* must be entered as a multiple of 4.

Command Modes

CONFIGURATION

Command History

Version 9.4.(0.0)	Added support for PBR.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Save the new CAM settings to the startup-config (`write-mem` or `copy run start`) then reload the system for the new settings to take effect.

The total amount of space allowed is 16 FP Blocks. System flow requires three blocks; these blocks cannot be reallocated. The `ipv4acl` profile range is from 1 to 4.

When configuring space for IPv6 ACLs, the total number of Blocks must equal 13.

On the MXL 10/40GbE switch IO module, there can be only one odd number of Blocks in the CLI configuration; the other Blocks must be in factors of two. For example, a CLI configuration of 5+4+2+1+1 Blocks is not supported; a configuration of 6+4+2+1 Blocks is supported.

Ranges for the CAM profiles are from 1 to 10, except for the `ipv6acl` profile which is from 0 to 10. The `ipv6acl` allocation must be a factor of two (2, 4, 6, 8, 10).

cam-optimization

Optimize CAM utilization for QoS Entries by minimizing require policy-map CAM space.

Syntax

```
cam-optimization [qos]
```

Parameters

qos	Optimize CAM usage for QoS.

Defaults: Disabled.

Command Modes: CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

When you enable this command, if a Policy Map containing classification rules (ACL and/or dscp/ ip-precedence rules) is applied to more than one physical interface on the same port pipe, only a single copy of the policy is written (only one FP entry is used).

NOTE: An ACL itself may still require more that a single FP entry, regardless of the number of interfaces. For more information, refer to the *IP Access Control Lists*, *Prefix Lists*, and *Route-map*sections in the *Dell Operating System Configuration Guide*.

show cam-acl

Display the details of the CAM profiles on the chassis and all stack units.

Syntax

```
show cam-acl
```

Defaults: none

Command Modes: EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The display reflects the settings implemented with the `cam-acl` command.

Example (Default)

```
Dell#show cam-acl (Default)

-- Chassis Cam ACL --
             Current Settings(in block sizes)
                   1 block = 128 entries
L2Acl        :         6
Ipv4Acl      :         4
Ipv6Acl      :         0
Ipv4Qos      :         2
L2Qos        :         1
L2PT         :         0
IpMacAcl     :         0
VmanQos      :         0
VmanDualQos  :         0
EcfmAcl      :         0
FcoeAcl      :         0
iscsiOptAcl  :         0
ipv4pbr      :         0
vrfv4Acl     :         0
Openflow     :         0
fedgovacl    :         0

-- stack-unit 0 --
           Current Settings(in block sizes)
                   1 block = 128 entries
L2Acl        :         6
Ipv4Acl      :         4
Ipv6Acl      :         0
Ipv4Qos      :         2
L2Qos        :         1
L2PT         :         0
IpMacAcl     :         0
VmanQos      :         0
VmanDualQos  :         0
EcfmAcl      :         0
FcoeAcl      :         0
iscsiOptAcl  :         0
ipv4pbr      :         0
vrfv4Acl     :         0
Openflow     :         0
fedgovacl    :         0
```

Example (Non-Default)

```
Dell#show cam-acl

-- Chassis Cam ACL --
           Current Settings(in block sizes)
L2Acl      :       2
Ipv4Acl    :       2
Ipv6Acl    :       2
Ipv4Qos    :       2
L2Qos      :       2
L2PT       :       1
IpMacAcl   :       2
VmanQos    :       0
VmanDualQos:       0
Ipv4pbr    :       0

-- Line card 4 --
Current Settings(in block sizes)
```

```
L2Acl       :       5
Ipv4Acl     :       5
Ipv6Acl     :       1
Ipv4Qos     :       1
L2Qos       :       1
L2PT        :       0
IpMacAcl    :       0
VmanQos     :       0
VmanDualQos:        0
Ipv4pbr     :       0

Dell#
```

show cam-acl-egress

Display the details of the FP groups allocated for the egress ACL.

Syntax

```
show cam-acl-egress
```

Defaults

none

Command Modes

Configuration

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The display reflects the settings implemented with the `cam-acl-egress` command.

Example

```
Dell#show cam-acl-egress

-- Chassis Egress Cam ACL --
          Current Settings(in block sizes)
L2Acl     :       1
Ipv4Acl   :       1
Ipv6Acl   :       2

-- Stack unit 0 --
          Current Settings(in block sizes)
L2Acl     :       1
Ipv4Acl   :       1
Ipv6Acl   :       2

Dell#
```

11

Control Plane Policing (CoPP)

The CoPP commands are supported on the Dell Networking MXL 10/40GbE Switch IO Module.

control-plane-cpuqos

To manage control-plane traffic, enter control-plane mode and configure the switch.

Syntax `control-plane-cpuqos`

Defaults Not configured.

Command Modes CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

service-policy rate-limit-cpu-queues

Apply a policy map for the system to rate limit control traffic on a per-queue basis.

Syntax `service-policy rate-limit-cpu-queues` *`policy-name`*

Parameters

policy-name	Enter the service-policy name, using a string up to 32 characters.

Defaults Not configured.

Command Modes CONTROL-PLANE-CPUQOS

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Create a policy-map by associating a queue number with the qos-policy.

Create QoS policies prior to enabling this command.

For CoPP, do not use the keywords `cpu-qos` when creating qos-policy-input.

Related Commands	qos-policy-input — creates a QoS input policy map. policy-map-input — creates an input policy map.

service-policy rate-limit-protocols

Apply a policy for the system to rate limit control protocols on a per-protocol basis.

Syntax

```
service-policy rate-limit-protocols policy-name
```

Parameters

policy-name	Enter the service-policy name, using a string up to 32 characters.

Defaults	Not configured.
Command Modes	CONTROL-PLANE-CPUQOS

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

This command applies the service-policy based on the type of protocol defined in the ACL rules.

Create ACL and QoS policies prior to enabling this command.

For CoPP, do not use the keywords `cpu-qos` when creating qos-policy-input.

Related Commands

ip access-list extended — creates an extended IP ACL.

mac access-list extended — creates an extended MAC ACL.

qos-policy-input — creates a QoS input policy map.

class-map — creates a QoS class map.

policy-map-input — creates an input policy map.

show cpu-queue rate cp

Display the rates for each queue.

Syntax

```
show cpu-queue rate cp
```

Defaults	Not configured.

Command Modes EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information This command applies the service-policy based on the type of protocol defined in the ACL rules.

Create ACL and QoS policies prior to enabling this command.

Example

```
Dell#show cpu-queue rate cp
 Service-Queue          Rate (PPS)      Burst ()
 --------------         -----------      -----------
Q0                         1300            512
Q1                         300             50
Q2                         300             50
Q3                         400             50
Q4                         2000            50
Q5                         300             50
Q6                         400             50
Q7                         400             50
Q8                         400             50
Q9                         600             50
Q10                        300             50
Q11                        300             50
```

show ip protocol-queue-mapping

Display the queue mapping for each configured protocol.

Syntax `show ip protocol-queue-mapping`

Defaults Not configured.

Command Modes EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show ip protocol-queue-mapping
 Protocol   Src-Port   Dst-Port   TcpFlag  Queue   EgPort
Rate (kbps)
 --------   --------   --------   -------  -----   ------
-----------
TCP (BGP)     any/179    179/any    _        Q9
_           _
UDP (DHCP)    67/68      68/67      _        Q10
_           _
UDP (DHCP-R)  67         67         _        Q10
_           _
TCP (FTP)     any        21         _        Q6
_           _
ICMP          any        any        _        Q6
_           _
```

```
IGMP          any        any        _        Q11
_           _
TCP (MSDP)    any/639    639/any    _        Q11
_           _
UDP (NTP)     any        123        _        Q6
_           _
OSPF          any        any        _        Q9
_           _
PIM           any        any        _        Q11
_           _
UDP (RIP)     any        520        _        Q9
_           _
TCP (SSH)     any        22         _        Q6
_           _
TCP (TELNET)  any        23         _        Q6
_           _
VRRP          any        any        _        Q10
_           _
Dell#
```

show ipv6 protocol-queue-mapping

Display the queue mapping for each configured IPv6 protocol.

Syntax `show ipv6 protocol-queue-mapping`

Defaults Not configured.

Command Modes EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show ipv6 protocol-queue-mapping
 Protocol   Src-Port   Dst-Port   TcpFlag  Queue   EgPort
Rate (kbps)
 --------   --------   --------   -------  -----   ------
-----------
TCP (BGP)     any/179    179/any    _        Q9
_           _
ICMPV6 NA     any        any        _        Q6
_           _
ICMPV6 RA     any        any        _        Q6
_           _
ICMPV6 NS     any        any        _        Q5
_           _
ICMPV6 RS     any        any        _        Q5
_           _
ICMPV6        any        any        _        Q6
_           _
VRRPV6        any        any        _        Q10
_           _
OSPFV3        any        any        _        Q9
_           _
Dell#
```

show mac protocol-queue-mapping

Display the queue mapping for the MAC protocols.

Syntax	`show mac protocol-queue-mapping`
Defaults	Not configured.
Command Modes	EXEC Privilege
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show mac protocol-queue-mapping
 Protocol     Destination Mac       EtherType   Queue
EgPort     Rate (kbps)
 --------     ---------------       ---------   -----
------     -----------
ARP           any                   0x0806      Q5/
Q6           CP
FRRP          01:01:e8:00:00:10/11  any
Q7              CP
LACP          01:80:c2:00:00:02     0x8809
Q7              CP
LLDP          any                   0x88cc
Q8              CP
GVRP          01:80:c2:00:00:21     any
Q8              CP
STP           01:80:c2:00:00:00     any
Q7              CP
ISIS          01:80:c2:00:00:14/15  any
Q9              CP
              09:00:2b:00:00:04/05  any
Q9              CP
Dell#
```

12

Data Center Bridging (DCB)

Data center bridging (DCB) refers to a set of IEEE Ethernet enhancements that provide data centers with a single, robust, converged network to support multiple traffic types, including local area network (LAN), server, and storage traffic.

The Dell Networking Operating System (OS) commands for data center bridging features include 802.1Qbb priority-based flow control (PFC), 802.1Qaz enhanced transmission selection (ETS), and the data center bridging exchange (DCBX) protocol.

advertise dcbx-appln-tlv

On a DCBX port with a manual role, configure the application priority TLVs advertised on the interface to DCBX peers.

Syntax

`advertise dcbx-appln-tlv {fcoe | iscsi}`

To remove the application priority TLVs, use the `no advertise dcbx-appln-tlv {fcoe | iscsi}` command.

Parameters

{fcoe | iscsi}	Enter the application priority TLVs, where: • `fcoe`: enables the advertisement of FCoE in application priority TLVs. • `iscsi`: enables the advertisement of iSCSI in application priority TLVs.

Defaults

Application priority TLVs are enabled to advertise FCoE and iSCSI.

Command Modes

PROTOCOL LLDP

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To disable TLV transmission, use the `no` form of the command; for example, `no advertise dcbx-appln-tlv iscsi`.

advertise dcbx-tlv

On a DCBX port with a manual role, configure the PFC and ETS TLVs advertised to DCBX peers.

Syntax	`advertise dcbx-tlv {ets-conf | ets-reco | pfc} [ets-conf | ets-reco | pfc] [ets-conf | ets-reco | pfc]` To remove the advertised ETS TLVs, use the `no advertise dcbx-tlv` command.
Parameters	**{ets-conf | ets-reco | pfc}** — Enter the PFC and ETS TLVs advertised, where: • `ets-conf`: enables the advertisement of ETS configuration TLVs. • `ets-reco`: enables the advertisement of ETS recommend TLVs. • `pfc`: enables the advertisement of PFC TLVs.
Defaults	All PFC and ETS TLVs are advertised.
Command Modes	PROTOCOL LLDP
Command History	**Version 9.2(0.0)** — Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only. **Version 8.3.16.1** — Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	You can configure the transmission of more than one TLV type at a time; for example: `advertise dcbx-tlv ets-conf ets-reco`. You can enable ETS recommend TLVs (`ets-reco`) only if you enable ETS configuration TLVs (`ets-conf`). To disable TLV transmission, use the `no` form of the command; for example, `no advertise dcbx-tlv pfc ets-reco`. DCBX requires that you enable LLDP to advertise DCBX TLVs to peers. Configure DCBX operation at the INTERFACE level on a switch or globally on the switch. To verify the DCBX configuration on a port, use the `show interface dcbx detail` command.

bandwidth-percentage

Configure the bandwidth percentage allocated to priority traffic in port queues.

Syntax	`bandwidth-percentage` *`percentage`* To remove the configured bandwidth percentage, use the `no bandwidth-percentage` command.

Parameters	*percentage*	(Optional) Enter the bandwidth percentage. The percentage range is from 1 to 100% in units of 1%.

Defaults none

Command Modes QOS-POLICY-OUT-ETS

Command History	**Version 9.2(0.0)**	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

By default, equal bandwidth is assigned to each port queue and each dot1p priority in a priority group. To configure bandwidth amounts in associated dot1p queues, use the `bandwidth-percentage` command. When specified bandwidth is assigned to some port queues and not to others, the remaining bandwidth (100% minus assigned bandwidth amount) is equally distributed to unassigned nonstrict priority queues in the priority group. The sum of the allocated bandwidth to all queues in a priority group must be 100% of the bandwidth on the link.

ETS-assigned bandwidth allocation applies only to data queues, not to control queues.

The configuration of bandwidth allocation and strict-queue scheduling is not supported at the same time for a priority group. If you configure both, the configured bandwidth allocation is ignored for priority-group traffic when you apply the output policy on an interface.

By default, equal bandwidth is assigned to each priority group in the ETS output policy applied to an egress port if you did not configure bandwidth allocation. The sum of configured bandwidth allocation to dot1p priority traffic in all ETS priority groups must be 100%. Allocate at least 1% of the total bandwidth to each priority group and queue. If bandwidth is assigned to some priority groups but not to others, the remaining bandwidth (100% minus assigned bandwidth amount) is equally distributed to nonstrict-priority groups which have no configured scheduler.

Related Commands

- qos-policy-output ets — creates a QoS output policy.
- scheduler — schedules priority traffic in port queues.

dcb-enable

Enable data center bridging.

Syntax `dcb enable`

To disable DCB, use the `no dcb enable` command.

Defaults none

Command Modes CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information DCB is not supported if you enable `link-level flow control` on one or more interfaces.

dcb-input

To apply pause or flow control for specified priorities using a configure delay time, create a DCB input policy.

Syntax `dcb-input` *`policy-name`*

To delete the DCB input policy, use the `no dcb-input` command.

Parameters

policy-name	Maximum: 32 alphanumeric characters.

Defaults none

Command Modes CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

As soon as you apply a DCB policy with PFC enabled on an interface, DCBx starts exchanging information with PFC-enabled peers. The IEEE802.1Qbb, CEE, and CIN versions of PFC TLV are supported. DCBx also validates PFC configurations received in TLVs from peer devices.

By applying a DCB input policy with PFC enabled, you enable PFC operation on ingress port traffic. To achieve complete lossless handling of traffic, also enable PFC on all DCB egress ports or configure the dot1p priority-queue assignment of PFC priorities to lossless queues (refer to `pfc no-drop queues`).

To remove a DCB input policy, including the PFC configuration it contains, enter the `no dcb-input` *`policy-name`* command in Interface Configuration mode.

NOTE: Please note that Dell Networking does not recommended to use this command as it has been deprecated in the current 9.4(0.0) release. A warning message appears when you try to run this command indicating that you have to use the `dcb-map` commands in the future.

Related Commands	dcb-policy input — applies the input policy with the PFC configuration.

dcb-output

To associate an ETS configuration with priority traffic, create a DCB output policy.

Syntax

`dcb-output policy-name`

To remove the ETS output policy globally, use the `no dcb output policy-name` command.

Parameters

policy-name	Enter the DCB output policy name. The maximum is 32 alphanumeric characters.

Defaults

none

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To associate a priority group with an ETS output policy with scheduling and bandwidth configuration, create a DCB output policy. You can apply a DCB output policy on multiple egress ports. When you apply an ETS output policy on an interface, ETS-configured scheduling and bandwidth allocation take precedence over any configured settings in QoS output policies.

The ETS configuration associated with 802.1 priority traffic in a DCB output policy is used in DCBX negotiation with ETS peers.

NOTE: Please note that Dell Networking does not recommended to use this command as it has been deprecated in the current 9.4(0.0) release. A warning message appears when you try to run this command indicating that you have to use the `dcb-map` commands in the future.

Related Commands

dcb-policy output — applies the output policy.

dcb-policy buffer-threshold (Global Configuration)

Assign the DCB policy to the DCB buffer threshold profile on stack ports that applies globally throughout the system.

Syntax

```
dcb-policy buffer-threshold stack-unit all stack-ports all
profile-name
```

Parameters

dcb-buffer-threshold	Configure the profile name for the DCB buffer threshold.
profile-name	Enter the name of the profile, which can be a string of up to 32 characters in length.
stack-unit all	Enter the stack unit identification. Indicates the specific the stack unit or units. Entering all shows the status for all stacks.
stack-port all	Enter the port number of a port in a switch stack.

Default None

Command Modes CONFIGURATION mode

Command History

Version 9.3(0.0)	Introduced on the MXL platform.

Usage Information

You can configure up to a maximum of four lossless (PFC) queues. By configuring four lossless queues, you can configure four different priorities and assign a particular priority to each application that your network is used to process. For example, you can assign a higher priority for time-sensitive applications and a lower priority for other services, such as file transfers. You can configure the amount of buffer space to be allocated for each priority and the pause or resume thresholds for the buffer. This method of configuration enables you to effectively manage and administer the behavior of lossless queues.

Example

```
Dell(conf)# dcb-policy buffer-threshold stack-unit all stack-
ports all test
```

dcb-policy buffer-threshold (Interface Configuration)

Assign the DCB policy to the DCB buffer threshold profile on interfaces. This setting takes precedence over the global buffer-threshold setting.

Syntax

```
dcb-policy buffer-threshold profile-name
```

Parameters

buffer-threshold	Configure the profile name for the DCB buffer threshold
profile-name	Enter the name of the profile, which can be a string of up to 32 characters in length.

Default	None
Command Modes	INTERFACE mode
Command History	**Version 9.3(0.0)** Introduced on the MXL platform.
Usage Information	You can configure a maximum of four lossless (PFC) queues. By configuring four lossless queues, you can configure four different priorities and assign a particular priority to each application that your network is used to process. For example, you can assign a higher priority for time-sensitive applications and a lower priority for other services, such as file transfers. You can configure the amount of buffer space to be allocated for each priority and the pause or resume thresholds for the buffer. This method of configuration enables you to effectively manage and administer the behavior of lossless queues.
Example	`Dell(conf-if-te-0/0)#dcb-policy buffer-threshold test`

dcb-policy input

Apply the input policy with the PFC configuration to an ingress interface.

Syntax

`dcb-policy input` *`policy-name`*

To delete the input policy, use the `no dcb-policy input` command.

Parameters

policy-name	Enter the input policy name with the PFC configuration to an ingress interface.

Defaults

none

Command Modes

INTERFACE

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

If you apply an input policy with PFC disabled (`no pfc mode on`):

- You can enable link-level flow control on the interface. To delete the input policy, first disable link-level flow control. PFC is then automatically enabled on the interface because an interface is by default PFC-enabled.
- PFC still allows you to configure lossless queues on a port to ensure no-drop handling of lossless traffic.

When you apply an input policy to an interface, an error message is displayed if:

- The PFC dot1p priorities result in more than two lossless port queues globally on the switch.
- You already enabled link-level flow control. PFC and link-level flow control cannot be enabled at the same time on an interface.

In a switch stack, configure all stacked ports with the same PFC configuration.

A DCB input policy for PFC applied to an interface may become invalid if you reconfigure the dot1p-queue mapping. This situation occurs when the new dot1p-queue assignment exceeds the maximum number (2) of lossless queues supported globally on the switch. In this case, all PFC configurations received from PFC-enabled peers are removed and resynchronized with the peer devices.

Traffic may be interrupted when you reconfigure PFC no-drop priorities in an input policy or reapply the policy to an interface.

NOTE: Please note that Dell Networking does not recommended to use this command as it has been deprecated in the current 9.4.(0.0) release. A warning message appears when you try to run this command indicating that you have to use the `dcb-map` commands in the future.

Related Commands

dcb-input — creates a DCB input policy.

dcb-policy input stack-unit stack-ports all

Apply the specified DCB input policy on all ports of the switch stack or a single stacked switch.

Syntax

`dcb-policy input stack-unit {all | *stack-unit-id*} stack-ports all *dcb-input-policy-name*`

To remove all DCB input policies applied to the stacked ports and rest the PFC to its default settings, use the `no dcb-policy input stack-unit all` command.

To remove only the DCB input policies applied to the specified switch, use the `no dcb-policy input stack-unit` command.

Parameters

stack-unit-id	Enter the stack unit identification.
dcb-input-policy-name	Enter the policy name for the DCB input policy.

Defaults

none

Command Modes

CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The `dcb-policy input stack-unit all` command overwrites any previous `dcb-policy input stack-unit stack-unit-id` configurations. Similarly, a `dcb-policy input stack-unit stack-unit-id` command overwrites any previous `dcb-policy input stack-unit all` configuration.

NOTE: Please note that Dell Networking does not recommended to use this command as it has been deprecated in the current 9.4.(0.0) release. A warning message appears when you try to run this command indicating that you have to use the `dcb-map` commands in the future.

Related Commands

dcb-policy output stack-unit stack-ports all — applies the specified DCB output policy.

dcb-policy output

Apply the output policy with the ETS configuration to an egress interface.

Syntax

`dcb-policy output *policy-name*`

To delete the output policy, use the `no dcb-policy output` command.

Parameters

policy-name	Enter the output policy name.

Defaults

none

Command Modes

INTERFACE

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

When you apply an ETS output policy to on interface, ETS-configured scheduling and bandwidth allocation take precedence over any configured settings in QoS output policies.

To remove an ETS output policy from an interface, use the `no dcb-policy output policy-name` command. ETS is enabled by default with the default ETS configuration applied (all dot1p priorities in the same group with equal bandwidth allocation).

NOTE: Please note that Dell Networking does not recommended to use this command as it has been deprecated in the current 9.4(0.0) release. A warning message appears when you try to run this command indicating that you have to use the `dcb-map` commands in the future.

Related Commands	[dcb-output](#) — creates a DCB output policy.

dcb-policy output stack-unit stack-ports all

Apply the specified DCB output policy on all ports of the switch stack or a single stacked switch.

Syntax

```
dcb-policy output stack-unit {all | stack-unit-id} stack-ports
all dcb-output-policy-name
```

To remove all DCB output policies applied to the stacked ports, use the `no dcb-policy output stack-unit all` command.

To remove only the DCB output policies applied to the specified switch, use the `no dcb-policy output stack-unit` command.

Parameters

stack-unit-id	Enter the stack unit identification.
dcb-output-policy-name	Enter the policy name for the DCB output policy.

Defaults

none

Command Modes

CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The `dcb-policy output stack-unit all` command overwrites any previous `dcb-policy output stack-unit stack-unit-id` configurations. Similarly, a `dcb-policy output stack-unit stack-unit-id` command overwrites any previous `dcb-policy output stack-unit all` configuration.

You can apply a DCB output policy with ETS configuration to all stacked ports in a switch stack or an individual stacked switch. You can apply different DCB output policies to different stack units.

NOTE: Please note that Dell Networking does not recommended to use this command as it has been deprecated in the current 9.4.(0.0) release. A warning message appears when you try to run this command indicating that you have to use the `dcb-map` commands in the future.

Related Commands

[dcb-policy input stack-unit stack-ports all](#) — applies the specified DCB input policy.

dcb stack-unit all pfc-buffering pfc-port-count pfc-queues

Configure the PFC buffer for all switches in the stack.

Syntax

`dcb stack-unit all pfc-buffering pfc-port-count {1-56} pfc-queues {1-2}`

To remove the configuration for the PFC buffer on all switches in the stack, use the `no dcb stack-unit all pfc-buffering pfc-port-count pfc-queues` command.

Parameters

pfc-port-count *{1-56}*	Enter the pfc-port count. The range is 1 to 56.
pfc-queues *{1-2}*	Enter the pfc-queue number. The range is 1 to 2.

Defaults

The PFC buffer is enabled on all ports on the stack unit.

Command Modes

CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

If you configure PFC on a 40GbE port, count the 40GbE port as four PFC-enabled ports in the pfc-port number you enter in the command syntax.

To achieve lossless PFC operation, the PFC port count and queue number used for the reserved buffer size that is created must be greater than or equal to the buffer size required for PFC-enabled ports and lossless queues on the switch.

You must reload the stack or a specified stack unit (use the reload command in EXEC Privilege mode) for the PFC buffer configuration to take effect.

Related Commands

dcb stack-unit pfc-buffering pfc-port pfc-queues – configures the PFC buffer for all port pipes in a specified stack unit.

dcb stack-unit pfc-buffering pfc-port-count pfc-queues

Configure the PFC buffer for all port pipes in a specified stack unit by specifying the port-pipe number, number of PFC-enabled ports, and number of configured lossless queues.

Syntax

`dcb stack-unit stack-unit-id [port-set port-set-id] pfc-buffering pfc-ports {1-56} pfc-queues {1-2}`

To remove the configuration for the PFC buffer on all port pipes in a specified stack unit, use the `no dcb stack-unit` *`stack-unit-id`* `[port-set` *`port-set-id`*`] pfc-buffering pfc-ports pfc-queues` command.

Parameters

stack-unit-id	Enter the stack unit identification. The range is from 0 to 5.
port-set	Enter the port-set identification. The only valid port-set ID (port-pipe number) on an MXL Switch is 0.
pfc-ports *{1-56}*	Enter the pfc-ports. The range is from 1 to 56.
pfc-queues *{1-2}*	Enter the pfc-queue number. The range is from 1 to 2.

Command Modes CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

If you configure PFC on a 40GbE port, count the 40GbE port as four PFC-enabled ports in the pfc-port number you enter in the command syntax.

To achieve lossless PFC operation, the PFC port count and queue number used for the reserved buffer size that is created must be greater than or equal to the buffer size required for PFC-enabled ports and lossless queues on the switch.

You must reload the stack or a specified stack unit (use the `reload` command in EXEC Privilege mode) for the PFC buffer configuration to take effect.

Related Commands

dcb stack-unit pfc-buffering pfc-port pfc-queues — configures the PFC buffer for all switches in the stack.

dcbx port-role

Configure the DCBX port role the interface uses to exchange DCB information.

Syntax

```
dcbx port-role {config-source | auto-downstream | auto-upstream
| manual}
```

To remove DCBX port role, use the `no dcbx port-role {config-source | auto-downstream | auto-upstream | manual}` command.

Parameters

config-source | auto-downstream | auto-upstream | manual	Enter the DCBX port role, where: • `config-source`: configures the port to serve as the configuration source on the switch. • `auto-upstream`: configures the port to receive a peer configuration. The configuration source is elected from auto-upstream ports. • `auto-downstream`: configures the port to accept the internally propagated DCB configuration from a configuration source. • `manual`: configures the port to operate only on administer-configured DCB parameters. The port does not accept a DCB configuration received form a peer or a local configuration source.

Defaults

Manual

Command Modes

INTERFACE PROTOCOL LLDP

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

DCBX requires that you enable LLDP to advertise DCBX TLVs to peers.

Configure DCBX operation at the INTERFACE level on a switch or globally on the switch. To verify the DCBX configuration on a port, use the `show interface dcbx detail` command.

dcbx version

Configure the DCBX version used on the interface.

Syntax

```
dcbx version {auto | cee | cin | ieee-v2.5}
```

To remove the DCBX version, use the `dcbx version {auto | cee | cin | ieee-v2.5}` command.

Parameters

auto | cee | cin | ieee-v2.5	Enter the DCBX version type used on the interface, where: • `auto`: configures the port to operate using the DCBX version received from a peer. • `cee`: configures the port to use CDD (Intel 1.01). • `cin`: configures the port to use Cisco-Intel-Nuova (DCBX 1.0).

- `ieee-v2`: configures the port to use IEEE 802.1az (Draft 2.5).

Defaults	**Auto**	
Command Modes	INTERFACE PROTOCOL LLDP	
Command History	Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

DCBX requires that you enable LLDP to advertise DCBX TLVs to peers.

Configure DCBX operation at the INTERFACE level on a switch or globally on the switch. To verify the DCBX configuration on a port, use the `show interface dcbx detail` command.

debug dcbx

Enable DCBX debugging.

Syntax

```
debug dcbx {all | auto-detect-timer | config-exchng | fail |
mgmt | resource | sem | tlv}
```

To disable DCBX debugging, use the `no debug dcbx` command.

Parameters

{all | auto-detect-timer | config-exchng | fail | mgmt | resource | sem | tlv}	Enter the type of debugging, where: • `all`: enables all DCBX debugging operations. • `auto-detect-timer`: enables traces for DCBX auto-detect timers. • `config-exchng`: enables traces for DCBX configuration exchanges. • `fail`: enables traces for DCBX failures. • `mgmt`: enables traces for DCBX management frames. • `resource`: enables traces for DCBX system resource frames. • `sem`: enables traces for the DCBX state machine. • `tlv`: enables traces for DCBX TLVs.

Defaults none

Command Modes

EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

description

Enter a text description of the DCB policy (PFC input or ETS output).

Syntax

```
description text
```

To remove the text description, use the `no description` command.

Parameters

text	Enter the description of the output policy. The maximum is 32 characters.

Defaults

none

Command Modes

- DCB INPUT POLICY
- DCB OUTPUT POLICY

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

- dcb-input — creates a DCB PFC input policy.
- dcb-policy input — applies the output policy.
- dcb-output — creates a DCBETS output policy.
- dcb-policy output — applies the output policy.

ets mode on

Enable the ETS configuration so that scheduling and bandwidth allocation configured in an ETS output policy or received in a DCBX TLV from a peer can take effect on an interface.

Syntax

```
ets mode on
```

To remove the ETS configuration, use the `no ets mode on` command.

Defaults

ETS mode is on.

Command Modes

DCB OUTPUT POLICY

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

If you disable ETS in an output policy applied to an interface using the `no ets mode on` command, any previously configured QoS settings at the interface or global level takes effect. If you configure QoS settings at the interface or global level and in an output policy map (the `service-policy output` command), the QoS configuration in the output policy takes precedence.

NOTE: Please note that Dell Networking does not recommended to use this command as it has been deprecated in the current 9.4(0.0) release. A warning message appears when you try to run this command indicating that you have to use the `dcb-map` commands in the future.

Related Commands

- dcb-output — creates a DCB output policy.
- dcb-policy output — applies the output policy.

fcoe priority-bits

Configure the FCoE priority advertised for the FCoE protocol in application priority TLVs.

Syntax

`fcoe priority-bits` *`priority-bitmap`*

To remove the configured FCoE priority, use the `no fcoe priority-bits` command.

Parameters

priority-bitmap	Enter the priority-bitmap range. The range is from 1 to FF.

Defaults

0x8

Command Modes

PROTOCOL LLDP

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information	This command is available at the global level only.

iscsi priority-bits

Configure the iSCSI priority advertised for the iSCSI protocol in application priority TLVs.

Syntax

`iscsi priority-bits` *`priority-bitmap`*

To remove the configured iSCSI priority, use the `no iscsi priority-bits` command.

Parameters

priority-bitmap	Enter the priority-bitmap range. The range is from 1 to FF.

Defaults	0x10
Command Modes	PROTOCOL LLDP

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information	This command is available at the global level only.

priority

Configure the priority for the PFC threshold to be allocated to the buffer space parameters.

Syntax

`priority` *`value`* `buffer-size` *`size`* `pause-threshold` *`threshold-value`* `resume-offset` *`threshold-value`* `shared-threshold-weight` *`size`*

Parameters

priority	Specify the priority of the queue for which the buffer space settings apply
value	Enter a number in the range of 0 to 7 to denote the priority to be allocated to the dynamic buffer control mechanism
buffer-size	Ingress buffer size
size	Size of the ingress buffer in KB. Enter a number in the range of 0 to 7787. The default is 45 KB.
pause-threshold	Buffer limit for pause frames to be sent

threshold-value	Buffer limit at which the port sends the pause to peer in KB. Enter a number in the range of 0 to 7787. The default is 10 KB.
resume-offset	Buffer offset limit for resuming in KB
threshold-value	Buffer offset limit at which the port resumes the peer in KB. Enter a number in the range of 1 to 7787. The default is 10 KB.
shared-threshold-weight	Buffer shared threshold weight
size	Weightage of the priorities on the shared buffer size in the system. Enter a number in the range of 0 to 9. The default shared threshold weight is 10.

Default

The default size of the ingress buffer is 45 KB. The default buffer limit at which the port sends the pause to peer and recommences the sending of packets to the peer is 10 KB. The default threshold weight of the shared buffer space is 10.

Command Modes

DCB-BUFFER-THRESHOLD mode

Command History

Version 9.3(0.0)	Introduced on the MXL platform.

Usage Information

For each priority, you can specify the shared buffer threshold limit, the ingress buffer size, buffer limit for pausing the acceptance of packets, and the buffer offset limit for resuming the acceptance of received packets. When PFC detects congestion on a queue for a specified priority, it sends a pause frame for the 802.1p priority traffic to the transmitting device.

You can use the`priority` command to set up both the administrative and peer-related PFC priorities. For example, you can configure the intended buffer configuration for all 8 priorities. If you configure the number of lossless queues as 4 and if the administrator-configured priorities configured within the DCB input policy is applied, then the configuration for those priorities are pre-designed. However, if the peer-provided priorities are applied, although a DCB input policy is present, the peer-provided priorities become effective for buffer configuration. This method of configuration provides an easy and flexible technique to accommodate both administratively-configured and peer-configured priorities.

Example

```
Dell (conf-dcb-buffer-thr)#priority 0 buffer-size 52 pause-
threshold 16 resume-offset 10 shared-threshold-weight 7
```

pfc link-delay

Configure the link delay used to pause specified priority traffic.

Syntax

`pfc link-delay value`

To remove the link delay, use the `no pfc link-delay` command.

Parameters

value	The range is (in quanta) from 712 to 65535. One quantum is equal to a 512-bit transmission.

Defaults

45556 quantum

Command Modes

DCB INPUT POLICY

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The minimum link delay must be greater than the round-trip transmission time a peer must honor a PFC pause frame multiplied by the number of PFC-enabled ingress ports.

Related Commands

dcb-input — creates a DCB input policy.

pfc mode on

Enable the PFC configuration on the port so that the priorities are included in DCBX negotiation with peer PFC devices.

Syntax

`pfc mode on`

To disable the PFC configuration, use the `no pfc mode on` command.

Defaults

PFC mode is on.

Command Modes

DCB INPUT POLICY

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

By applying a DCB input policy with PFC enabled, you enable PFC operation on ingress port traffic. To achieve complete lossless handling of traffic, also enable

PFC on all DCB egress ports or configure the dot1p priority-queue assignment of PFC priorities to lossless queues (refer to `pfc no-drop queues`).

To disable PFC operation on an interface, enter the `no pfc mode on` command in DCB Input Policy Configuration mode. PFC is enabled and disabled as global DCB operation is enabled (`dcb-enable`) or disabled (`no dcb-enable`).

You cannot enable PFC and link-level flow control at the same time on an interface.

Related Commands	dcb-input — creates a DCB input policy.

pfc no-drop queues

Configure the port queues that still function as no-drop queues for lossless traffic.

Syntax

`pfc no-drop queues` *`queue-range`*

To remove the no-drop port queues, use the `no pfc no-drop queues` command.

Parameters

queue-range	Enter the queue range. Separate the queue values with a comma; specify a priority range with a dash; for example, `pfc no-drop queues 1,3` or `pfc no-drop queues 2-3`. The range is from 0 to 3.

Defaults

No lossless queues are configured.

Command Modes

INTERFACE

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The maximum number of lossless queues globally supported on the switch is two.

- The following lists the dot1p priority-queue assignments.

dot1p Value in the Incoming Frame	Description heading
0	0
1	0

dot1p Value in the Incoming Frame	Description heading
2	0
3	1
4	2
5	3
6	3
7	3

pfc priority

Configure the CoS traffic to be stopped for the specified delay.

Syntax

`pfc priority` *`priority-range`*

To delete the pfc priority configuration, use the `no pfc priority` command.

Parameters

priority-range	Enter the 802.1p values of the frames to be paused. Separate the priority values with a comma; specify a priority range with a dash; for example, pfc priority 1,3,5-7. The range is from 0 to 7.

Defaults

none

Command Modes

DCB INPUT POLICY

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

You can enable any number of 802.1p priorities for PFC. Queues to which PFC priority traffic is mapped are lossless by default. Traffic may be interrupted due to an interface flap (going down and coming up) when you reconfigure the lossless queues for no-drop priorities in a PFC input policy and reapply the policy to an interface.

The maximum number of lossless queues supported on the I/O Aggregator switch is four.

A PFC peer must support the configured priority traffic (as DCBX detects) to apply PFC.

NOTE: Please note that Dell Networking does not recommended to use this command as it has been deprecated in the current 9.4(0.0) release. A warning message appears when you try to run this command indicating that you have to use the `dcb-map` commands in the future.

Related Commands	dcb-input — creates a DCB input policy.

priority-group

To use with an ETS output policy, create an ETS priority group.

Syntax

`priority-group group-name`

To remove the priority group, use the `no priority-group` command.

Parameters

group-name	Enter the name of the ETS priority group. The maximum is 32 characters.

Defaults none

Command Modes CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

A priority group consists of 802.1p priority values that are grouped for similar bandwidth allocation and scheduling, and that share latency and loss requirements. All 802.1p priorities mapped to the same queue must be in the same priority group.

You must configure 802.1p priorities in priority groups associated with an ETS output policy. You can assign each dot1p priority to only one priority group.

The maximum number of priority groups supported in ETS output policies on an interface is equal to the number of data queues (4) on the port. The 802.1p priorities in a priority group can map to multiple queues.

If you configure more than one priority queue as strict priority or more than one priority group as strict priority, the higher numbered priority queue is given preference when scheduling data traffic.

NOTE: Please note that Dell Networking does not recommended to use this command as it has been deprecated in the current 9.4(0.0) release. A warning message appears when you try to run this command indicating that you have to use the `dcb-map` commands in the future.

Related Commands	• priority-list — configures the 802.1p priorities for an ETS output policy. • set-pgid — configures the priority-group.

priority-group qos-policy

Associate the 802.1p priority traffic in a priority group with the ETS configuration in a QoS output policy.

Syntax

`priority-group group-name qos-policy ets-policy-name`

To remove the 802.1p priority group, use the `no priority-group qos-policy` command.

Parameters

group-name	Enter the group name of the 802.1p priority group. The maximum is 32 characters.
ets-policy-name	Enter the ETS policy name.

Defaults

none

Command Modes

DCB OUTPUT POLICY

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The ETS configuration associated with 802.1p priority traffic in a DCB output policy is used in DCBX negotiation with ETS peers.

If you disable ETS in an output policy applied to an interface using the `no ets mode on` command, any previously configured QoS settings at the interface or global level take effect. If you configure QoS settings at the interface or global level and in an output policy map (the `service-policy output` command), the QoS configuration in the output policy takes precedence.

> NOTE: Please note that Dell Networking does not recommended to use this command as it has been deprecated in the current 9.4(0.0) release. A warning message appears when you try to run this command indicating that you have to use the `dcb-map` commands in the future.

Related Commands

- dcb-output — creates a DCB output policy.
- dcb-policy output — applies the output policy.

priority-list

Configure the 802.1p priorities for the traffic on which you want to apply an ETS output policy.

Syntax

`priority-list value`

To remove the priority list, use the `no priority-list` command.

Parameters

value	Enter the priority list value. Separate priority values with a comma; specify a priority range with a dash; for example, priority-list 3,5-7. The range is from 0 to 7.

Defaults

none

Command Modes

PRIORITY-GROUP

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

By default:

- All 802.1p priorities are grouped in priority group 0.
- 100% of the port bandwidth is assigned to priority group 0. The complete bandwidth is equally assigned to each priority class so that each class has 12 to 13%.

  NOTE: Please note that Dell Networking does not recommended to use this command as it has been deprecated in the current 9.4(0.0) release. A warning message appears when you try to run this command indicating that you have to use the `dcb-map` commands in the future.

Related Commands

- priority-group qos-policy — associates an ETS priority group with an ETS output policy.
- set-pgid — configures the priority-group.

qos-policy-output ets

To configure the ETS bandwidth allocation and scheduling for priority traffic, create a QoS output policy.

Syntax

`qos-policy-output policy-name ets`

To remove the QoS output policy, use the `no qos-policy-output ets` command.

Parameters

policy-name	Enter the policy name. The maximum is 32 characters.

Command Modes	CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

If an error occurs in an ETS output-policy configuration, the configuration is ignored and the scheduler and bandwidth allocation settings are reset to the ETS default values (all priorities are in the same ETS priority group and bandwidth is allocated equally to each priority).

If an error occurs when a port receives a peer's ETS configuration, the port's configuration is reset to the previously configured ETS output policy. If no ETS output policy was previously applied, the port is reset to the default ETS parameters.

Related Commands

- scheduler — schedules the priority traffic in port queues.
- bandwidth-percentage — bandwidth percentage allocated to the priority traffic in port queues.

scheduler

Configure the method used to schedule priority traffic in port queues.

Syntax

`scheduler` *`value`*

To remove the configured priority schedule, use the `no scheduler` command.

Parameters

value	Enter schedule priority value. The valid values are: • `strict`: strict-priority traffic is serviced before any other queued traffic. • `werr`: weighted elastic round robin (werr) provides low-latency scheduling for priority traffic on port queues.

Defaults

Weighted elastic round robin (WERR) scheduling is used to queue priority traffic.

Command Modes

POLICY-MAP-OUT-ETS

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

dot1p priority traffic on the switch is scheduled to the current queue mapping. dot1p priorities within the same queue must have the same traffic properties and scheduling method.

ETS-assigned scheduling applies only to data queues, not to control queues.

The configuration of bandwidth allocation and strict-queue scheduling is not supported at the same time for a priority group. If you configure both, the configured bandwidth allocation is ignored for priority-group traffic when you apply the output policy on an interface.

Related Commands

- qos-policy-output ets — configures the ETS bandwidth allocation.
- bandwidth-percentage — bandwidth percentage allocated to priority traffic in port queues.

set-pgid

Configure the priority-group identifier.

Syntax

`set-pgid value`

To remove the priority group, use the `no set-pgid` command.

Parameters

value	Enter the priority group identification. The range is from 0 to 7.

Defaults

none

Command Modes

PRIORITY-GROUP

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

NOTE: Please note that Dell Networking does not recommended to use this command as it has been deprecated in the current 9.4(0.0) release. A warning message appears when you try to run this command indicating that you have to use the `dcb-map` commands in the future.

Related Commands

- priority-group qos-policy — creates an ETS priority group.

- priority-list — configures the 802.1p priorities.

show dcb

Displays the data center bridging status, the number of PFC-enabled ports, and the number of PFC-enabled queues.

Syntax	`show dcb [stack-unit unit-number]`

Parameters

unit number	Enter the DCB unit number. The range is from 0 to 5.

Command Modes	EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information	Specify a stack-unit number on the Master switch in a stack.

Example

```
Dell(conf)#do show  dcb
stack-unit 0 port-set 0
DCB Status         :Enabled
PFC Queue Count    :2
Total Buffer[lossy + lossless] (in KB):7982
PFC Total Buffer (in KB)              :5872
PFC Shared Buffer (in KB)             :832
PFC Available Buffer (in KB)          :4860
Dell (conf)#
```

show interface dcbx detail

Displays the DCBX configuration on an interface.

Syntax	`show interface port-type slot/port dcbx detail`

Parameters

port-type	Enter the port type.
slot/port	Enter the slot/port number.

Command Modes	CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To clear DCBX frame counters, use the `clear dcbx counters interface` *`stack-unit/port`* command.

The following describes the `show interface dcbx detail` command shown in the following example.

Field	Description
Interface	Interface type with chassis slot and port number.
Port-Role	Configured the DCBX port role: auto-upstream, auto-downstream, config-source, or manual.
DCBX Operational Status	Operational status (enabled or disabled) used to elect a configuration source and internally propagate a DCB configuration. The DCBX operational status is the combination of PFC and ETS operational status.
Configuration Source	Specifies whether the port serves as the DCBX configuration source on the switch: true (yes) or false (no).
Local DCBX Compatibility mode	DCBX version accepted in a DCB configuration as compatible. In auto-upstream mode, a port can only receive a DCBX version supported on the remote peer.
Local DCBX Configured mode	DCBX version configured on the port: CEE, CIN, IEEE v2.5, or Auto (port auto-configures to use the DCBX version received from a peer).
Peer Operating version	DCBX version that the peer uses to exchange DCB parameters.
Local DCBX TLVs Transmitted	Transmission status (enabled or disabled) of advertised DCB TLVs (see TLV code at the top of the show command output).
Local DCBX Status: DCBX Operational Version	DCBX version advertised in Control TLVs.
Local DCBX Status: DCBX Max Version Supported	Highest DCBX version supported in Control TLVs.
Local DCBX Status: Sequence Number	Sequence number transmitted in Control TLVs.

Field	Description
Local DCBX Status: Acknowledgment Number	Acknowledgement number transmitted in Control TLVs.
Local DCBX Status: Protocol State	Current operational state of the DCBX protocol: ACK or IN-SYNC.
Peer DCBX Status: DCBX Operational Version	DCBX version advertised in Control TLVs received from the peer device.
Peer DCBX Status: DCBX Max Version Supported	Highest DCBX version supported in Control TLVs received from the peer device.
Peer DCBX Status: Sequence Number	Sequence number transmitted in Control TLVs received from the peer device.
Peer DCBX Status: Acknowledgment Number	Acknowledgement number transmitted in Control TLVs received from the peer device.
Total DCBX Frames transmitted	Number of DCBX frames sent from the local port.
Total DCBX Frames received	Number of DCBX frames received from the remote peer port.
Total DCBX Frame errors	Number of DCBX frames with errors received.
Total DCBX Frames unrecognized	Number of unrecognizable DCBX frames received.

Example

```
Dell(conf)# show interface tengigabitethernet 0/49 dcbx detail
Dell#show interface te 0/49 dcbx detail

E-ETS Configuration TLV enabled
  e-ETS Configuration TLV disabled
R-ETS Recommendation TLV enabled
  r-ETS Recommendation TLV disabled
P-PFC Configuration TLV enabled
  p-PFC Configuration TLV disabled
F-Application priority for FCOE enabled
  f-Application Priority for FCOE disabled
I-Application priority for iSCSI enabled
  i-Application Priority for iSCSI disabled
-----------------------------------------------------------

Interface TenGigabitEthernet 0/49
  Remote Mac Address 00:00:00:00:00:11
   Port Role is Auto-Upstream
  DCBX Operational Status is Enabled
  Is Configuration Source? TRUE

Local DCBX Compatibility mode is CEE
  Local DCBX Configured mode is CEE
  Peer Operating version is CEE
  Local DCBX TLVs Transmitted: ErPfi

Local DCBX Status
-----------------
  DCBX Operational Version is 0
  DCBX Max Version Supported is 0
  Sequence Number: 2
  Acknowledgment Number: 2
  Protocol State: In-Sync

Peer DCBX Status:
----------------
  DCBX Operational Version is 0
  DCBX Max Version Supported is 255
  Sequence Number: 2
  Acknowledgment Number: 2
  Total DCBX Frames transmitted 27
  Total DCBX Frames received 6
  Total DCBX Frame errors 0
  Total DCBX Frames unrecognized 0
```

show interface ets

Displays the ETS configuration applied to egress traffic on an interface, including priority groups with priorities and bandwidth allocation.

Syntax

`show interface port-type slot/port ets {summary | detail}`

Parameters

port-type slot/ port ets	Enter the port-type slot and port ETS information.
{summary | detail}	Enter the keyword `summary` for a summary list of results or enter the keyword `detail` for a full list of results.

Command Modes

CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To clear ETS TLV counters, use the `clear ets counters interface` *`port-type slot/port`* command.

The following describes the `show interface summary` command shown in the following example.

Field	Description
Interface	Interface type with stack-unit and port number.
Max Supported TC Group	Maximum number of priority groups supported.
Number of Traffic Classes	Number of 802.1p priorities currently configured.
Admin mode	ETS mode: on or off. When on, the scheduling and bandwidth allocation configured in an ETS output policy or received in a DCBX TLV from a peer can take effect on an interface.
Admin Parameters	ETS configuration on local port, including priority groups, assigned dot1p priorities, and bandwidth allocation.
Remote Parameters	ETS configuration on remote peer port, including admin mode (enabled if a valid TLV was received or disabled), priority groups, assigned dot1p priorities, and bandwidth allocation. If ETS admin mode is enabled on the remote port for DCBX exchange, the Willing bit received in ETS TLVs from the remote peer is included.
Local Parameters	ETS configuration on local port, including admin mode (enabled when a valid TLV is received from a peer), priority groups, assigned dot1p priorities, and bandwidth allocation.
Operational status (local port)	Port state for current operational ETS configuration: • `Init`: Local ETS configuration parameters were exchanged with the peer. • `Recommend`: Remote ETS configuration parameters were received from the peer. • `Internally propagated`: ETS configuration parameters were received from the configuration source.
ETS DCBX Oper status	Operational status of the ETS configuration on the local port: match or mismatch.
State Machine Type	Type of state machine used for DCBX exchanges of ETS parameters: Feature — for legacy DCBX versions; Asymmetric — for an IEEE version.
Conf TLV Tx Status	Status of ETS Configuration TLV advertisements: enabled or disabled.
ETS TLV Statistic: Input Conf TLV pkts	Number of ETS Configuration TLVs received.

Field	Description
ETS TLV Statistic: Output Conf TLV pkts	Number of ETS Configuration TLVs transmitted.
ETS TLV Statistic: Error Conf TLV pkts	Number of ETS Error Configuration TLVs received.

Example (Summary)

```
Dell(conf)# show interfaces te 0/0 ets summary
Interface TenGigabitEthernet 0/0
Max Supported TC Groups is 4
Number of Traffic Classes is 8
Admin mode is on
Admin Parameters:
------------------
Admin is enabled
TC-grp Priority#        Bandwidth TSA
0      0,1,2,3,4,5,6,7  100%      ETS
1                         0%      ETS
2                         0%      ETS
3                         0%      ETS
4                         0%      ETS
5                         0%      ETS
6                         0%      ETS
7                         0%      ETS
Priority#              Bandwidth  TSA
0                        13%      ETS
1                        13%      ETS
2                        13%      ETS
3                        13%      ETS
4                        12%      ETS
5                        12%      ETS
6                        12%      ETS
7                        12%      ETS
Remote Parameters:
-------------------
Remote is disabled
Local Parameters:
------------------
Local is enabled
TC-grp Priority#        Bandwidth TSA
0      0,1,2,3,4,5,6,7  100%      ETS
1                         0%      ETS
2                         0%      ETS
3                         0%      ETS
4                         0%      ETS
5                         0%      ETS
6                         0%      ETS
7                         0%      ETS
Priority#               Bandwidth TSA
0                        13%      ETS
1                        13%      ETS
2                        13%      ETS
3                        13%      ETS
4                        12%      ETS
5                        12%      ETS
6                        12%      ETS
7                        12%      ETS
Oper status is init
```

```
Conf TLV Tx Status is disabled
Traffic Class TLV Tx Status is disabled
```

Example (Detail)

```
Dell(conf)# show interfaces tengigabitethernet 0/0 ets detail
Interface TenGigabitEthernet 0/0
Max Supported TC Groups is 4
Number of Traffic Classes is 8
Admin mode is on
Admin Parameters :
------------------
Admin is enabled
TC-grp Priority#        Bandwidth TSA
0      0,1,2,3,4,5,6,7  100%      ETS
1                       0%        ETS
2                       0%        ETS
3                       0%        ETS
4                       0%        ETS
5                       0%        ETS
6                       0%        ETS
7                       0%        ETS

Priority#               Bandwidth TSA
0                       13%       ETS
1                       13%       ETS
2                       13%       ETS
3                       13%       ETS
4                       12%       ETS
5                       12%       ETS
6                       12%       ETS
7                       12%       ETS
Remote Parameters:
-------------------
Remote is disabled

Local Parameters :
------------------
Local is enabled
TC-grp Priority#        Bandwidth TSA
0      0,1,2,3,4,5,6,7  100%      ETS
1                       0%        ETS
2                       0%        ETS
3                       0%        ETS
4                       0%        ETS
5                       0%        ETS
6                       0%        ETS
7                       0%        ETS

Priority#               Bandwidth TSA
0                       13%       ETS
1                       13%       ETS
2                       13%       ETS
3                       13%       ETS
4                       12%       ETS
5                       12%       ETS
6                       12%       ETS
7                       12%       ETS
Oper status is init
Conf TLV Tx Status is disabled
Traffic Class TLV Tx Status is disabled
0 Input Conf TLV Pkts, 0 Output Conf TLV Pkts, 0 Error Conf
TLV Pkts
0 Input Traffic Class TLV Pkts, 0 Output Traffic Class TLV
Pkts, 0 Error Traffic Class
```

```
TLV
Pkts
```

show interface pfc

Displays the PFC configuration applied to ingress traffic on an interface, including priorities and link delay.

Syntax `show interface port-type slot/port pfc {summary | detail}`

Parameters

port-type slot/ port pfc	Enter the port-type slot and port PFC information.
{summary | detail}	Enter the keyword `summary` for a summary list of results or enter the keyword `detail` for a full list of results.

Command Modes INTERFACE

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To clear the PFC TLV counters, use the `clear pfc counters interface` *`port-type slot/port`* command.

The following describes the `show interface pfc summary` command shown in the following example.

Field	Description
Interface	Interface type with stack-unit and port number.
Admin mode is on Admin is enabled	PFC admin mode is on or off with a list of the configured PFC priorities. When the PFC admin mode is on, PFC advertisements are enabled to be sent and received from peers; received PFC configuration take effect. The admin operational status for a DCBX exchange of PFC configuration is enabled or disabled.
Remote is enabled, Priority list Remote Willing Status is enabled	Operational status (enabled or disabled) of peer device for DCBX exchange of PFC configuration with a list of the configured PFC priorities. Willing status of peer device for DCBX exchange (Willing bit received in PFC TLV): enabled or disable.
Local is enabled	DCBX operational status (enabled or disabled) with a list of the configured PFC priorities.

Field	Description
Operational status (local port)	Port state for current operational PFC configuration: • `Init`: Local PFC configuration parameters were exchanged with the peer. • `Recommend`: Remote PFC configuration parameters were received from the peer. • `Internally propagated`: PFC configuration parameters were received from the configuration source.
PFC DCBX Oper status	Operational status for the exchange of the PFC configuration on the local port: match (up) or mismatch (down).
State Machine Type	Type of state machine used for DCBX exchanges of the PFC parameters: Feature — for legacy DCBX versions; Symmetric — for an IEEE version.
TLV Tx Status	Status of the PFC TLV advertisements: enabled or disabled.
PFC Link Delay	Link delay (in quanta) used to pause specified priority traffic.
Application Priority TLV: FCOE TLV Tx Status	Status of FCoE advertisements in application priority TLVs from the local DCBX port: enabled or disabled.
Application Priority TLV: SCSI TLV Tx Status	Status of ISCSI advertisements in application priority TLVs from the local DCBX port: enabled or disabled.
Application Priority TLV: Local FCOE Priority Map	Priority bitmap the local DCBX port uses in FCoE advertisements in application priority TLVs.
Application Priority TLV: Local ISCSI Priority Map	Priority bitmap the local DCBX port uses in ISCSI advertisements in application priority TLVs.
Application Priority TLV: Remote FCOE Priority Map	Status of FCoE advertisements in application priority TLVs from the remote peer port: enabled or disabled.
Application Priority TLV: Remote ISCSI Priority Map	Status of iSCSI advertisements in application priority TLVs from the remote peer port: enabled or disabled.
PFC TLV Statistics: Input TLV pkts	Number of PFC TLVs received.
PFC TLV Statistics: Output TLV pkts	Number of PFC TLVs transmitted.

Field	Description
PFC TLV Statistics: Error pkts	Number of PFC error packets received.
PFC TLV Statistics: Pause Tx pkts	Number of PFC pause frames transmitted.
PFC TLV Statistics: Pause Rx pkts	Number of PFC pause frames received.

Example (Summary)

```
Dell# show interfaces tengigabitethernet 0/49 pfc summary
Interface TenGigabitEthernet 0/49
  Admin mode is on
  Admin is enabled
  Remote is enabled, Priority list is 4
  Remote Willing Status is enabled
  Local is enabled
  Oper status is Recommended
  PFC DCBX Oper status is Up
  State Machine Type is Feature
  TLV Tx Status is enabled
  PFC Link Delay 45556 pause quantams
  Application Priority TLV Parameters :
  --------------------------------------
  FCOE TLV Tx Status is disabled
  ISCSI TLV Tx Status is disabled
  Local FCOE PriorityMap is 0x8
  Local ISCSI PriorityMap is 0x10
  Remote FCOE PriorityMap is 0x8
  Remote ISCSI PriorityMap is 0x8

Dell# show interfaces tengigabitethernet 0/49 pfc detail
  Interface TenGigabitEthernet 0/49
  Admin mode is on
  Admin is enabled
  Remote is enabled
  Remote Willing Status is enabled
  Local is enabled
  Oper status is recommended
  PFC DCBX Oper status is Up
  State Machine Type is Feature
  TLV Tx Status is enabled
  PFC Link Delay 45556 pause quanta
  Application Priority TLV Parameters :
  --------------------------------------
  FCOE TLV Tx Status is disabled
  ISCSI TLV Tx Status is disabled
  Local FCOE PriorityMap is 0x8
  Local ISCSI PriorityMap is 0x10
  Remote FCOE PriorityMap is 0x8
  Remote ISCSI PriorityMap is 0x8
  0 Input TLV pkts, 1 Output TLV pkts, 0 Error pkts,
  0 Pause Tx pkts, 0 Pause Rx pkts
```

show interface pfc statistics

Displays counters for the PFC frames received and transmitted (by dot1p priority class) on an interface.

Syntax

```
show interface port-type slot/port pfc statistics
```

Parameters

port-type	Enter the port type.
slot/port	Enter the slot/port number.

Command Modes

INTERFACE

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example (Summary)

```
Dell#show interfaces te 0/3 pfc statistics
Interface TenGigabitEthernet 0/3

Priority Rx XOFF Frames Rx Total Frames Tx Total Frames
-------------------------------------------------------
0        0              0               0
1        0              0               0
2        0              0               0
3        0              0               0
4        0              0               0
5        0              0               0
6        0              0               0
7        0              0               0
```

show qos dcb-input

Displays the PFC configuration in a DCB input policy.

Syntax

```
show qos dcb-input [pfc-profile]
```

Parameters

pfc-profile	Enter the PFC profile.

Command Modes

CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information	NOTE: Please note that Dell Networking does not recommended to use this command as it has been deprecated in the current 9.4(0.0) release. A warning message appears when you try to run this command indicating that you have to use the `dcb-map` commands in the future.

Example

```
Dell(conf)# show qos dcb-input
dcb-input pfc-profile
  pfc link-delay 32
  pfc priority 0-1
dcb-input pfc-profile1
  no pfc mode on
  pfc priority 6-7
```

show qos dcb-output

Displays the ETS configuration in a DCB output policy.

Syntax

```
show qos dcb-output [ets-profile]
```

Parameters

[ets-profile]	Enter the ETS profile.

Command Modes EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

NOTE: Please note that Dell Networking does not recommended to use this command as it has been deprecated in the current 9.4(0.0) release. A warning message appears when you try to run this command indicating that you have to use the `dcb-map` commands in the future.

Example

```
Dell# show qos dcb-output
dcb-output ets
  priority-group san qos-policy san
  priority-group ipc qos-policy ipc
  priority-group lan qos-policy lan
```

show qos priority-groups

Displays the ETS priority groups configured on the switch, including the 802.1p priority classes and ID of each group.

Syntax `show qos priority-groups`

Command Modes EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

> **NOTE:** Please note that Dell Networking does not recommended to use this command as it has been deprecated in the current 9.4(0.0) release. A warning message appears when you try to run this command indicating that you have to use the `dcb-map` commands in the future.

Example

```
Dell#show qos priority-groups
priority-group ipc
  priority-list 4
  set-pgid 2
```

show stack-unit stack-ports ets details

Displays the ETS configuration applied to egress traffic on stacked ports, including ETS Operational mode on each unit and the configurated priority groups with dot1p priorities, bandwidth allocation, and scheduler type.

Syntax `show stack-unit {all | *stack-unit*} stack-ports {all | *port-number*} ets details`

Parameters

stack-unit	Enter the stack unit identification.
port-number	Enter the port number.

Command Modes CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell(conf)# show stack-unit all stack-ports all ets details

Stack unit 0 stack port all
```

```
Max Supported TC Groups is 4
Number of Traffic Classes is 1
Admin mode is on

Admin Parameters:
--------------------
Admin is enabled
TC-grp Priority#        Bandwidth TSA
------------------------------------------------
0      0,1,2,3,4,5,6,7  100%      ETS
1                       - -
2                       - -
3                       - -
4                       - -
5                       - -
6                       - -
7                       - -
8                       - -

Stack unit 1 stack port all
Max Supported TC Groups is 4
Number of Traffic Classes is 1
Admin mode is on
Admin Parameters:
--------------------
Admin is enabled
TC-grp Priority#        Bandwidth TSA
------------------------------------------------
0      0,1,2,3,4,5,6,7  100%      ETS
1                       -         -
2                       -         -
3                       -         -
4                       -         -
5                       -         -
6                       -         -
7                       -         -
8                       -         -
```

dcb pfc-shared-buffer-size

Configure the maximum amount of shared buffer size for PFC packets in kilobytes.

You must configure the shared buffer size to be less than the total PFC buffer size. If the buffer size and DCB buffer threshold settings are applied on one or more ports, a validaiton is performed to determine whether following condition is satisfied: Shared-pfc-buffer-size <= (Total-pfc-buffer-size - Σpfc priority <> buffer-size on each port, priority).

If the preceding condition is not satisfied by the shared PFC buffer size value, the configuration is not saved and a system logging message is generated stating that the shared buffer size that you attempt to specify cannot be configured because of the existing total buffer space on the system being lower than the shared buffer size. You must either enter a smaller value for the shared buffer size or increase the total buffer size appropriately by using the `dcb pfc-total- buffer-size` command.

Syntax	`dcb pfc-shared—buffer—size` *`KB`*

Parameters	*KB*	Enter a number in the range of 0 to 7787.

Default None.

Command Modes CONFIGURATION mode

Command History	Version 9.3(0.0)	Introduced on the MXL platform.

Usage Information Configure the maximum shared buffer available for PFC traffic. You can choose to increase or decrease the shared buffer that is currently allocated in the system by default. You must configure the shared buffer size to be less than the total PFC buffer size. If the buffer size and DCB buffer threshold settings are applied on one or more ports, a validation is performed to determine whether following condition is satisfied:

Shared-pfc-buffer-size <= (Total-pfc-buffer-size - Σpfc priority <> buffer-size on each port, priority).

If the preceding condition is not satisfied by the shared PFC buffer size value, the configuration is not saved and a system logging message is generated as follows:

```
S4810-YU-MR-FTOS (conf)#dcb pfc-shared-buffer-size 2000
```

```
%ERROR: pfc shared buffer size configured cannot accommodate
existing buffer requirement in the system.
```

Example

```
Dell(conf)#dcb pfc-shared-buffer-size 5000
```

dcb-buffer-threshold

Configure the profile name for the DCB buffer threshold.

Syntax `dcb buffer—threshold` *`profile-name`*

Parameters	*profile-name*	Enter the name of the profile, which can be a string of up to 32 characters in length.

Default None

Command Modes CONFIGURATION mode

Command History	Version 9.3(0.0)	Introduced on the MXL platform.

Usage Information When you enter the profile name, you enter the DCB buffer threshold configuration mode. You can specify the shared buffer threshold limit, the ingress buffer size, buffer limit for pausing the acceptance of packets, and the buffer offset limit for resuming the acceptance of received packets.

Example	`Dell(conf)#dcb buffer—threshold test`

dcb enable pfc-queues

Configure the number of PFC queues.

Syntax

```
dcb enable pfc-queues value
```

Parameters

value	Enter the number of PFC queues. The range is from 1 to 4. The number of ports supported based on lossless queues configured will depend on the buffer.

Command Modes

CONFIGURATION mode

Command History

Version 9.3(0.0)	Supported on the MXL 10/40GbE Switch IO Module platform.

Usage Information

You can configure up to a maximum of four lossless (PFC) queues. By configuring four lossless queues, you can configure four different priorities and assign a particular priority to each application that your network is used to process. For example, you can assign a higher priority for time-sensitive applications and a lower priority for other services, such as file transfers. You can configure the amount of buffer space to be allocated for each priority and the pause or resume thresholds for the buffer. This method of configuration enables you to effectively manage and administer the behavior of lossless queues.

Example

```
Dell(conf)#dcb pfc-queues 4
```

dcb <ets | pfc> enable

Enable priority flow control or enhanced transmission selection on interface.

Syntax

```
dcb <ets | pfc> enablepfc >enable
```

- To disable ETS on interface, use "**no dcb ets enable**" command.
- To disable PFC on interface, use "**no dcb pfc enable**" command.

Defaults

Enable

Command Modes

INTERFACE

Command History

Version 9.3 (0.1)	Introduced on S6000, S4810, and S4820T.

Usage Information	PFC and ETS are enabled by default on the interfaces when DCB is globally enabled (refer to dcb enable). In some network topology, you may want to disable PFC on an interface and apply link level flow control; Similarly you may want to disable ETS on an interface and apply QoS bandwidth configurations.

Limitations

- “`dcb-map`” CLI on interface is mutually exclusive to “`no dcb ets enable`” and “`no dcb pfc enable`”.
- “`pfc priority`” CLI is mutually exclusive to “`no dcb pfc enable`” command.
- Deprecated CLI “`dcb-policy input`” and “`no dcb pfc enable`” cannot coexist at interface level.
- Deprecated CLI “`dcb-policy output`” and “`no dcb ets enable`” cannot coexist at interface level.

Related Commands

dcb-input—applies dcb-input profile on interface.

dcb-policy output—applies dcb-output profile on interface.

pfc priority—enable PFC on 802.1p priority traffic without using a dcb-map.

dcb-map—applies dcb-map profile on interface.

dcb-policy buffer-threshold (Interface Configuration)

Assign the DCB policy to the DCB buffer threshold profile on interfaces. This setting takes precedence over the global buffer-threshold setting.

Syntax `dcb-policy buffer-threshold profile-name`

Parameters

buffer-threshold	Configure the profile name for the DCB buffer threshold
profile-name	Enter the name of the profile, which can be a string of up to 32 characters in length.

Default	None
Command Modes	INTERFACE mode

Command History

Version 9.3(0.0)	Introduced on the MXL platform.

Usage Information

You can configure a maximum of four lossless (PFC) queues. By configuring four lossless queues, you can configure four different priorities and assign a particular priority to each application that your network is used to process. For example, you can assign a higher priority for time-sensitive applications and a lower priority for other services, such as file transfers. You can configure the amount of buffer space to be allocated for each priority and the pause or resume thresholds for the buffer. This method of configuration enables you to effectively manage and administer the behavior of lossless queues.

Example

```
Dell(conf-if-te-0/0)#dcb-policy buffer-threshold test
```

dcb-policy buffer-threshold (Global Configuration)

Assign the DCB policy to the DCB buffer threshold profile on stack ports that applies globally throughout the system.

Syntax

```
dcb-policy buffer-threshold stack-unit all stack-ports all
profile-name
```

Parameters

dcb-buffer-threshold	Configure the profile name for the DCB buffer threshold.
profile-name	Enter the name of the profile, which can be a string of up to 32 characters in length.
stack-unit all	Enter the stack unit identification. Indicates the specific the stack unit or units. Entering all shows the status for all stacks.
stack-port all	Enter the port number of a port in a switch stack.

Default

None

Command Modes

CONFIGURATION mode

Command History

Version 9.3(0.0)	Introduced on the MXL platform.

Usage Information

You can configure up to a maximum of four lossless (PFC) queues. By configuring four lossless queues, you can configure four different priorities and assign a particular priority to each application that your network is used to process. For example, you can assign a higher priority for time-sensitive applications and a lower priority for other services, such as file transfers. You can configure the amount of buffer space to be allocated for each priority and the pause or resume thresholds for the buffer. This method of configuration enables you to effectively manage and administer the behavior of lossless queues.

Example

```
Dell(conf)# dcb-policy buffer-threshold stack-unit all stack-
ports all test
```

pfc mode on

Enable the PFC configuration on the port so that the priorities are included in DCBX negotiation with peer PFC devices.

Syntax

`pfc mode on`

To disable the PFC configuration, use the `no pfc mode on` command.

Defaults

PFC mode is on.

Command Modes

DCB MAP

Command History

Version 9.3(0.0)	Introduced on the MXL 10/40GbE Switch with the FC Flex IO module.

Usage Information

By applying a DCB input policy with PFC enabled, you enable PFC operation on ingress port traffic. To achieve complete lossless handling of traffic, also enable PFC on all DCB egress ports or configure the dot1p priority-queue assignment of PFC priorities to lossless queues (refer to `pfc no-drop queues`).

To disable PFC operation on an interface, enter the `no pfc mode on` command in DCB Input Policy Configuration mode. PFC is enabled and disabled as global DCB operation is enabled (`dcb-enable`) or disabled (`no dcb-enable`).

You cannot enable PFC and link-level flow control at the same time on an interface.

NOTE: Please note that Dell Networking does not recommended to use this command as it has been deprecated in the current 9.4(0.0) release. A warning message appears when you try to run this command indicating that you have to use the `dcb-map` commands in the future.

priority-pgid

Assign 802.1p priority traffic to a priority group in a DCB map.

FC Flex IO Modules with MXL

Syntax

```
priority-pgid dot1p0_group-num dot1p1_group-num dot1p2_group-num dot1p3_group-num dot1p4_group-num dot1p5_group-num dot1p6_group-num dot1p7_group-num
```

Parameters

dot1p0_group-num	Enter the priority group number for each 802.1p class of traffic in a DCB map.

dot1p1_group-num

dot1p2_group-num

dot1p3_group-num

dot1p4_group-num

dot1p5_group-num

dot1p6_group-num

dot1p7_group-num

Defaults

None

Command Modes

DCB MAP

Command History

Version 9.3(0.0)	Introduced on the FC Flex IO module installed in the MXL 10/40GbE Switch module platform.

Usage Information

PFC and ETS settings are not pre-configured on Ethernet ports. You must use the `dcb-map` command to configure different groups of 802.1p priorities with PFC and ETS settings.

Using the `priority-pgid` command, you assign each 802.1p priority to one priority group. A priority group consists of 802.1p priority values that are grouped together for similar bandwidth allocation and scheduling, and that share latency and loss requirements. All 802.1p priorities mapped to the same queue must be in the same priority group. For example, the `priority-pgid 0 0 0 1 2 4 4 4` command creates the following groups of 802.1p priority traffic:

- Priority group 0 contains traffic with dot1p priorities 0, 1, and 2.
- Priority group 1 contains traffic with dot1p priority 3.
- Priority group 2 contains traffic with dot1p priority 4.
- Priority group 4 contains traffic with dot1p priority 5, 6, and 7.

To remove a priority-pgid configuration from a DCB map, enter the `no priority-pgid` command.

Related Commands

dcb-map — creates a DCB map to configure PFC and ETS parameters and applies the PFC and ETS settings on Ethernet ports.

priority-group bandwidth pfc— configures the ETS bandwidth allocation and the PFC setting used to manage the port traffic in an 802.1p priority group.

qos-policy-buffer

Create a QoS policy buffer and enter the configuration mode to configure the no-drop queues, ingress buffer size, buffer limit for pausing, and buffer offset limit for resuming.

Syntax

```
qos-policy-buffer queue queue-num pause no-drop queue buffer-size size pause-threshold threshold-value resume-offset threshold-value shared-threshold-weight size
```

Parameters

policy-name	Name of the QoS policy buffer that is applied to an interface for this setting to be effective in conjunction with the DCB input policy. You can specify the shared buffer threshold limit, the ingress buffer size, buffer limit for pausing the acceptance of packets, and the buffer offset limit for resuming the acceptance of received packets. This method of configuration enables different peer-provided and administrative priorities to be set up because the intended queue is directly configured instead of determining the priority to queue mapping for local and remote parameters.
queue 0 to queue 7	Specify the queue number to which the QoS policy buffer parameters apply
pause	Pause frames to be sent at the specified buffer limit levels and pause packet settings
no-drop	The packets for this queue must not be dropped
value	Enter a number in the range of 0 to 7 to denote the priority to be allocated to the dynamic buffer control mechanism
buffer-size	Ingress buffer size
size	Size of the ingress buffer in KB. Enter a number in the range of 0 to 7787. The default is 45 KB.
pause-threshold	Buffer limit for pause frames to be sent
threshold-value	Buffer limit at which the port sends the pause to peer in KB. Enter a number in the range of 0 to 7787. The default is 10 KB.
resume-offset	Buffer offset limit for resuming in KB
threshold-value	Buffer offset limit at which the port resumes the peer in KB. Enter a number in the range of 1 to 7787. The default is 10 KB.

shared-threshold-weight	Buffer shared threshold weight
size	Weightage of the priorities on the shared buffer size in the system. Enter a number in the range from 0 to 9. The default shared threshold weight is 10.

Default The default size of the ingress buffer is 45 KB. The default buffer limit at which the port sends the pause to peer and recommences the sending of packets to the peer is 10 KB. The default threshold weight of the shared buffer space is 10.

Command Modes DCB-BUFFER-THRESHOLD mode

Command History

Version 9.3(0.0)	Introduced on the MXL platform.

Usage Information You must apply this buffer policy at the interface level for the attributes to be applicable in conjunction with the DCB input policy.

For each QoS policy buffer, you can specify the shared buffer threshold limit, the ingress buffer size, buffer limit for pausing the acceptance of packets, and the buffer offset limit for resuming the acceptance of received packets. When PFC detects congestion on a queue for a specified priority, it sends a pause frame for the 802.1p priority traffic to the transmitting device.

You can use set up both the administrative and peer-related PFC priorities. For example, you can configure the intended buffer configuration for all 8 priorities. If you configure the number of lossless queues as 4 and if the administrator-configured priorities configured within the DCB input policy is applied, then the configuration for those priorities are pre-designed. However, if the peer-provided priorities are applied, although a DCB input policy is present, the peer-provided priorities become effective for buffer configuration. This method of configuration provides an easy and flexible technique to accommodate both administratively-configured and peer-configured priorities.

Example

```
Dell(conf)# qos-policy-buffer test
Dell (conf-qos-policy-buffer)#queue 0 pause no-drop buffer-size
128000 pause-threshold 103360 resume-threshold 83520

Dell(conf-qos-policy-buffer)# queue 4 pause no-drop buffer-size
128000 pause-threshold 103360 resume-threshold 83520
```

show qos dcb-map

Display the DCB parameters configured in a specified DCB map.

FC Flex IO Modules with MXL

Syntax	`show qos dcb-map map-name`

Parameters

map-name	Displays the PFC and ETS parameters configured in the specified map.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.3(0.0)	Introduced on the FC Flex IO module installed in the MXL 10/40GbE Switch.

Usage Information

Use the `show qos dcb-map` command to display the enhanced transmission selection (ETS) and priority-based flow control (PFC) parameters used to configure server-facing Ethernet ports.

The following table describes the `show qos dcb-map` output shown in the example below.

Field	Description
State	Complete: All mandatory DCB parameters are correctly configured. In progress: The DCB map configuration is not complete. Some mandatory parameters are not configured.
PFC Mode	PFC configuration in DCB map: On (enabled) or Off.
PG	Priority group configured in the DCB map.
TSA	Transmission scheduling algorithm used by the priority group: Enhanced Transmission Selection (ETS).
BW	Percentage of bandwidth allocated to the priority group.
PFC	PFC setting for the priority group: On (enabled) or Off.
Priorities	802.1p priorities configured in the priority group.

Example

```
Dell# show qos dcb-map dcbmap2

State   :Complete
PfcMode:ON
--------------------
PG:0 TSA:ETS  BW:50  PFC:OFF
Priorities:0 1 2 4 5 6 7
```

```
PG:1 TSA:ETS  BW:50  PFC:ON
Priorities:3
```

Related Commands

dcb-map — creates a DCB map to configure PFC and ETS parameters and applies the PFC and ETS settings on Ethernet ports.

show stack-unit stack-ports pfc details

Displays the PFC configuration applied to ingress traffic on stacked ports, including PFC Operational mode on each unit with the configured priorities, link delay, and number of pause packets sent and received.

Syntax

`show stack-unit {all | stack-unit} stack-ports {all | port-number} pfc details`

Parameters

stack-unit	Enter the stack unit.
port-number	Enter the port number.

Command Modes

CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell(conf)# show stack-unit all stack-ports all pfc details

stack unit 0 stack-port all
  Admin mode is On
  Admin is enabled, Priority list is 4-5
  Local is enabled, Priority list is 4-5
  Link Delay 45556 pause quantum
  0 Pause Tx pkts, 0 Pause Rx pkts

stack unit 1 stack-port all
  Admin mode is On
  Admin is enabled, Priority list is 4-5
  Local is enabled, Priority list is 4-5
  Link Delay 45556 pause quantum
  0 Pause Tx pkts, 0 Pause Rx pkts
```

13

Debugging and Diagnostics

The basic debugging and diagnostic commands are supported by the Dell Networking Operating System (OS).

This chapter contains the following sections:

- Offline Diagnostic Commands
- Buffer Tuning Commands
- Hardware Commands

Offline Diagnostic Commands

The offline diagnostics test suite is useful for isolating faults and debugging hardware. While tests are running, the Dell operating system results are saved as a text file (TestReport-SU-X.txt) in the flash directory. This `show file` command is available only on master and standby.

Important Points to Remember

- Offline diagnostics can only be run when the unit is offline.
- You can only run offline diagnostics on a unit to which you are connected via the console. In other words, you cannot run diagnostics on a unit to which you are connected to via a stacking link.
- Diagnostic results are printed to the screen. The Dell Networking OS does not write them to memory.
- Diagnostics only test connectivity, not the entire data path.

diag stack-unit

Run offline diagnostics on a stack unit.

Syntax

```
diag stack-unit number [alllevels | level0 | level1 | level2]
verbose no-reboot
```

Parameters

number	Enter the stack-unit number. The range is from 0 to 5.
alllevels	Enter the keyword `alllevels` to run the complete set of offline diagnostic tests.
level0	Enter the keyword `level0` to run Level 0 diagnostics. Level 0 diagnostics check for the presence of various components and perform essential path verifications. In addition, they verify the identification registers of the components on the board.

level1	Enter the keyword `Level1` to run Level 1 diagnostics. Level 1 diagnostics is a smaller set of diagnostic tests with support for automatic partitioning. They perform status/self test for all the components on the board and test their registers for appropriate values. In addition, they perform extensive tests on memory devices (for example, SDRAM, flash, NVRAM, EEPROM, and CPLD) wherever possible. There are no tests on 10G links. At this level, stack ports are shut down automatically.
level2	Enter the keyword `level2` to run Level 2 diagnostics. Level 2 diagnostics are a full set of diagnostic tests with no support for automatic partitioning. Level 2 diagnostics are used primarily for on-board loopback tests and more extensive component diagnostics. Various components on the board are put into Loopback mode and test packets are transmitted through those components. These diagnostics also perform snake tests using VLAN configurations. To test 10G links, physically remove the unit from the stack.
verbose	Enter the keyword `verbose` to run the diagnostic in Verbose mode. Verbose mode gives more information in the output than Standard mode.
no-reboot	Enter the keyword `no-reboot` to avoid automatic rebooting of the chassis after completion of diagnostic execution. Generally, this option is never used because if you run the diagnostic once again without rebooting the chassis, it may cause an issue with the diagnostic results..

Defaults none

Command Modes EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

offline stack-unit

Place a stack unit in the offline state.

Syntax `offline stack-unit number`

Parameters

number	Enter the stack-unit number. The range is from 0 to 5.

Defaults none

Command Modes EXEC Privilege

Command History		
	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The system reboots when the off-line diagnostics complete. This reboot is an automatic process. A warning message appears when the `offline stack-unit` command is implemented.

```
Warning - Diagnostic execution will cause stack-unit to reboot
after completion of diags.
```

```
Proceed with Offline-Diags [confirm yes/no]:y
```

online stack-unit

Place a stack unit in the online state.

Syntax `online stack-unit number`

Parameters

number	Enter the stack-unit number. The range is from 0 to 5.

Defaults none

Command Modes EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Buffer Tuning Commands

The following sections detail the buffer tuning commands.

WARNING: Altering the buffer allocations is a sensitive operation. Do not use any buffer tuning commands without first contacting the Dell Networking Technical Assistance Center (TAC).

buffer (Buffer Profile)

Allocate an amount of dedicated buffer space, dynamic buffer space, or packet pointers to queues 0 to 3.

Syntax

```
buffer [dedicated | dynamic | packets-pointers] queue0 number
queue1 number queue2 number queue3 number
```

Parameters

dedicated	Enter the keyword `dedicated` to configure the amount of dedicated buffer space per queue.

dynamic	Enter the keyword `dynamic` to configure the amount of dynamic buffer space per Field Processor.
packets-pointers	Enter the keywords `packets-pointers` to configure the number of packet pointers per queue.
queue0 *number*	Enter the keyword `queue0` and the number to allocate an amount of buffer space or packet pointers to Queue 0. • Dedicated Buffer Range: 0 to 2013. • Dynamic Buffer Range: FP: 0 to 2013. CSF: 0 to 131200 (in multiples of 80). • Packet Pointer Range: 0 to 2047.
queue1 *number*	Enter the keyword `queue1` and the number to allocate an amount of buffer space or packet pointers to Queue 1. • Dedicated Buffer Range: 0 to 2013. • Dynamic Buffer Range: FP: 0 to 2013. CSF: 0 to 131200 (in multiples of 80). • Packet Pointer Range: 0 to 2047.
queue2 *number*	Enter the keyword `queue2` and the number to allocate an amount of buffer space or packet pointers to Queue 2. • Dedicated Buffer Range: 0 to 2013. • Dynamic Buffer Range: FP: 0 to 2013. CSF: 0 to 131200 (in multiples of 80). • Packet Pointer Range: 0 to 2047.
queue3 *number*	Enter the keyword `queue3` and the number to allocate an amount of buffer space or packet pointers to Queue 3. • Dedicated Buffer Range: 0 to 2013. • Dynamic Buffer Range: FP: 0 to 2013. CSF: 0 to 131200 (in multiples of 80). • Packet Pointer Range: 0 to 2047.

Defaults	none
Command Modes	BUFFER PROFILE
Command History	Version 8.3.16.1 — Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	buffer-profile (Configuration) — creates a buffer profile that can be applied to an interface.

buffer (Configuration)

Apply a buffer profile to all Field or Switch Fabric processors in a port-pipe.

Syntax

```
buffer [csf | fp-uplink] port-set port-pipe buffer-policy
buffer-profile
```

Parameters

csf	Enter the keyword `csf` to apply a buffer profile to all Switch Fabric processors in a port-pipe.
fp-uplink	Enter the keyword `fp-uplink` to apply a buffer profile to all Field Processors in a a port-pipe.
port-set *port-pipe*	Enter the keywords `port-set` then the port-pipe number. The range is 0 to 1.
buffer-policy *buffer-profile*	Enter the keywords `buffer-policy` then the name of a buffer profile you created.

Defaults

none

Command Modes

BUFFER PROFILE

Command History

Version 8.3.16.10	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

If you attempt to apply a buffer profile to a non-existent port-pipe, the Dell Networking OS displays the following message. However, the configuration still appears in the running-config.

```
%DIFFSERV-2-DSA_BUFF_CARVING_INVALID_PORT_SET: Invalid FP port-
set 2 for stack-unit 2. Valid range of port-set is <0-1>
```

When you remove a buffer-profile using the `no buffer-profile [fp | csf]` command from CONFIGURATION mode, the buffer-profile name still appears in the output of `show buffer-profile [detail | summary]`. After a line card reset, the buffer profile correctly returns to the default values, but the profile name remains. Remove it from the `show buffer-profile [detail | summary]` command output by entering `no buffer [fp-uplink | csf] buffer-policy` from CONFIGURATION mode and `no buffer-policy` from INTERFACE mode.

Related Commands

buffer-profile (Configuration) — creates a buffer profile that can be applied to an interface.

buffer-profile (Configuration)

Create a buffer profile that can be applied to an interface.

Syntax `buffer-profile {fp | csf] profile-name {global {1Q | | 4q}`

Parameters

fp	Enter the keyword `fp` to create a buffer profile for the Field Processor.
csf	Enter the keyword `csf` to create a buffer profile for the Switch Fabric Processor.
profile-name	Create a name for the buffer profile,
global	Apply one of two pre-defined buffer profiles to all of the port-pipes in the system.
1Q	Enter the keyword `1Q` to choose a pre-defined buffer profile for single queue (for example, non-QoS) applications.
4Q	Enter the keyword `4q` to choose a pre-defined buffer profile for four queue (for example, QoS) applications.

Defaults Dynamic

Command Modes CONFIGURATION

Command History

Version 9.2(0.0)	Changed the default value from global 4Q to Dynamic.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The `buffer-profile global` command fails if you have already applied a custom buffer-profile on an interface. Similarly, when you configure `buffer-profile global`, you cannot not apply buffer-profile on any interface.

If the default buffer-profile is active, the Dell OS displays an error message instructing you to remove the default configuration using the `no buffer-profile global` command.

Reload the system for the global buffer-profile to take effect.

Related Commands

buffer (Buffer Profile) — allocates an amount of dedicated buffer space, dynamic buffer space, or packet pointers to queues from 0 to 3.

buffer-profile (Interface)

Apply a buffer profile to an interface.

Syntax	`buffer-profile profile-name`
Parameters	*profile-name* — Enter the name of the buffer profile you want to apply to the interface.
Defaults	none
Command Modes	INTERFACE
Command History	Version 8.3.16.1 — Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	buffer-profile (Configuration) – creates a buffer profile that can be applied to an interface.

show buffer-profile

Display the buffer profile that is applied to an interface.

Syntax	`show buffer-profile {detail | summary} {csf | fp-uplink}`
Parameters	detail — Display the buffer allocations of the applied buffer profiles. summary — Display the buffer-profiles that are applied to line card port-pipes in the system. csf — Display the Switch Fabric Processor buffer profiles that you have applied to line card port-pipes in the system. fp-uplink — Display the Field Processor buffer profiles that you have applied to line card port-pipes in the system.
Defaults	none
Command Modes	EXEC Privilege
Command History	Version 8.3.16.1 — Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show buffer-profile summary fp-uplink
Linecard  Port-set  Buffer-profile
0         0         test1
4         0         test2
Dell#
```

Related Commands

buffer-profile (Configuration) — Creates a buffer profile that can be applied to an interface.

show buffer-profile interface

Display the buffer profile that is applied to an interface.

Syntax

`show buffer-profile {detail | summary} interface *interface* *slot/port*`

Parameters

detail	Display the buffer allocations of a buffer profile.
summary	Display the Field Processors and Switch Fabric Processors that are applied to the system.
interface *interface*	Enter the keyword `interface` then the interface type, either `gigabitethernet` or `tengigabitethernet`.
slot/port	Enter the slot and port number of the interface.

Defaults

none

Command Modes

INTERFACE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show buffer-profile detail csf linecard 4 port-set 0
Linecard 4 Port-set 0
Buffer-profile test
Queue#  Dedicated Buffer   Buffer Packets
(Bytes)
0       36960              718
1       18560              358
2       18560              358
3       18560              358
4       9600               64
5       9600               64
6       9600               64
7       9600               63
Dell#
```

Related Commands

buffer-profile (Configuration) — creates a buffer profile that can be applied to an interface.

Hardware Commands

These commands display information from a hardware sub-component or ASIC.

clear hardware stack-unit

Clear statistics from selected hardware components.

Syntax

```
clear hardware stack-unit 0–5 {counters | unit 0–1 counters |
cpu data-plane statistics | cpu party-bus statistics | stack-
port 0–52}
```

Parameters

stack-unit *0–5*	Enter the keywords `stack-unit` then 0 to 5 to select a particular stack member and then enter one of the following command options to clear a specific collection of data.
counters	Enter the keyword `counters` to clear the counters on the selected stack member.
unit *0–0* counters	Enter the keyword `unit` along with a port-pipe number, from 0 to 1, then the keyword `counters` to clear the counters on the selected port-pipe.
cpu data-plane statistics	Enter the keywords `cpu data-plane statistics` to clear the data plane statistics.
cpu party-bus statistics	Enter the keywords `cpu party-bus statistics` to clear the management statistics.
stack-port *33–56*	Enter the keywords `stack-port` then the port number of the stacking port to clear the statistics of the particular stacking port. The range is from 33 to 56. NOTE: You can identify stack port numbers by physical inspection of the rear modules. The numbering is the same as for the 10G ports. You can also inspect the output of the `show system stack-ports` command.

Defaults

none

Command Modes

EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

show hardware stack-unit — displays the data plane or management plane input and output statistics of the designated component of the designated stack member.

clear hardware system-flow

Clear system-flow statistics from selected hardware components.

Syntax	`clear hardware system-flow layer2 stack-unit` *`0-5`* `port-set` *`0-0`* `counters`
Parameters	**stack-unit** ***0–5*** — Enter the keywords `stack-unit` then 0 to 5 to select a particular stack member and then enter one of the following command options to clear a specific collection of data. **port-set** ***0–0*** **counters** — Enter the keywords `port-set` along with a port-pipe number, then the keyword `counters` to clear the system-flow counters on the selected port-pipe.
Defaults	none
Command Modes	EXEC Privilege
Command History	**Version 8.3.16.1** — Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	show hardware stack-unit — displays the data plane or management plane input and output statistics of the designated component of the designated stack member.

show hardware layer2 acl

Display Layer 2 ACL or eg data for the selected stack member and stack member port-pipe.

Syntax	`show hardware layer2 acl stack-unit` *`0-5`* `port-set` *`0-0`*
Parameters	**stack-unit*0–5*** — Enter the keyword `stack-unit` then 0 to 5 to select a stack ID. **port-set** ***0–0*** — Enter the keywords `port-set` with a port-pipe number.
Defaults	none
Command Modes	EXEC Privilege
Command History	**Version 8.3.16.1** — Introduced on the MXL 10/40GbE Switch IO Module.

show hardware layer3

Display Layer 3 ACL or QoS data for the selected stack member and stack member port-pipe.

Syntax

```
show hardware layer3 {acl | qos} stack-unit 0–5 port-set 0–0
```

Parameters

acl | qos	Enter either the keyword `acl` or the keyword `qos` to select between ACL or QoS data.
stack-unit *0–5*	Enter the keywords `stack-unit` then a numeral from 0 to 5 to select a stack ID.
port-set *0–0*	Enter the keyword port-set with a port-pipe number.

Defaults none

Command Modes EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

show hardware stack-unit

Display the data plane or management plane input and output statistics of the designated component of the designated stack member.

Syntax

```
show hardware stack-unit 0–5 {buffer [buffer unit | port
[(1–56) | all] total buffer | buffer unit (1) port (1–56) queue
[(0–14) | all] buffer-info} {phy-firmware-version} {cpu data-
plane statistics [stack-port 0–52] | cpu party-bus statistics |
cpu private-mgmt statistics | drops [unit 0–1 [port 1–56]] |
stack-port 33–56 | unit 0–0 {counters | details | port-stats
[detail] | register}}
```

Parameters

stack-unit *0–5* {command-option}	Enter the keywords `stack-unit` then 0 to 5 to select a particular stack member and then enter one of the following command options to display a collection of data based on the option entered.
buffer	Enter the keyword `buffer`. To display the total buffer statistics for the stack unit, enter the keyword `total-buffer`. Enter the keywords `buffer unit` then `total-buffer` to display the buffer details per unit and mode of allocation. To display the forwarding plane statistics containing the packet buffer usage per port per stack unit, enter the keywords `buffer unit` then `port` and the port number (*1–56* or `all`), then `buffer-info`. To display the forwarding plane statistics containing the packet buffer statistics per COS per port, enter the keywords `buffer`

	`unit` and `port (`*`1-56`*`)`, and `queue` (*`0-14`* or `all`), and `buffer-info`. The buffer unit default is **1**.
phy-firmware-version	Each member of the stack is updated automatically with the latest firmware while booting as well as during OIR. To dump the physical firmware version for stack units, enter the keywords `phy-firmware-version`.
cpu data-plane statistics	(Optional) Enter the keywords `cpu data-plane statistics` then the keywords `stack port` and its number from 0 to 52 to display the data plane statistics, which shows the High Gig (Higig) port raw input/output counter statistics to which the stacking module is connected.
cpu party-bus statistics	Enter the keywords `cpu party-bus statistics`, to display the Management plane input/output counter statistics of the pseudo party bus interface.
cpu private-mgmt statistics	Enter the keywords `cpu private-mgmt statistics`, to display the Management plane input/output counter statistics of the Private Management interface.
drops [unit *0-0* [port *1-56*]]	Enter the keyword `drops` to display internal drops on the selected stack member. Optionally, use the keyword `unit` with 0 to select port-pipe 0, and then use `port `*`1-56`* to select a port on that port-pipe.
stack-port *33–56*	Enter the keywords `stack-port` and a stacking port number to select a stacking port for which to display statistics. Identify the stack port number as you would to identify a 10G port that was in the same place in one of the rear modules. NOTE: You can identify stack port numbers by physical inspection of the rear modules. The numbering is the same as for the 10G ports. You can also inspect the output of the `show system stack-ports` command.
unit *0–0* {counters | details | port-stats [detail] | register}	Enter the keyword `unit` then 0 for port-pipe 0, and then enter one of the following keywords to troubleshoot errors on the selected port-pipe and to give status on why a port is not coming up to register level: `counters`, `details`, `port-stats [detail]`, or `register`.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show hardware stack-unit 0 phy-firmware-version
PortNumber  Status   Programmed Version   SW Version
```

```
=====================================================
41          Present   01.06
01.06
42          Present   01.06
01.06
43          Present   01.06
01.06
44          Present   01.06
01.06
45          Present   01.06
01.06
46          Present   01.06
01.06
47          Present   01.06
01.06
48          Present   01.06
01.06
49          Not Present  N/A
N/A
Dell#
```

In the above example, the *Status* field represents presence of OPTM ports, *Programmed version*field represents loaded firmware version, and *SW version* represents the SDK version.

Example (data-plane)

```
Dell#show hardware stack-unit 0 cpu data-plane statistics

bc pci driver statistics for device:
rxHandle         :0
noMhdr           :0
noMbuf           :0
noClus           :0
recvd            :0
dropped          :0
recvToNet        :0
rxError          :0
rxDatapathErr    :0
rxPkt(COS0)      :0
rxPkt(COS1)      :0
rxPkt(COS2)      :0
rxPkt(COS3)      :0
rxPkt(COS4)      :0
rxPkt(COS5)      :0
rxPkt(COS6)      :0
rxPkt(COS7)      :0
rxPkt(UNIT0)     :0
transmitted      :1696
txRequested      :1696
noTxDesc         :0
txError          :0
txReqTooLarge    :0
txInternalError  :0
txDatapathErr    :0
txPkt(COS0)      :0
txPkt(COS1)      :0
txPkt(COS2)      :0
txPkt(COS3)      :0
txPkt(COS4)      :0
txPkt(COS5)      :0
txPkt(COS6)      :0
txPkt(COS7)      :0
txPkt(UNIT0)     :0
Dell#
```

Example

```
Dell#show hardware stack-unit 0 cpu party-bus statistics
Input Statistics:
  8189 packets, 8076608 bytes
  0 dropped, 0 errors
Output Statistics:
  366 packets, 133100 bytes
  0 errors
Dell#
```

Example (drops)

```
Dell#show hard stack-unit 0 drops
UNIT No: 0

Total Ingress Drops   : 7841475
Total IngMac Drops    : 0
Total Mmu Drops       : 0
Total EgMac Drops     : 0
Total Egress Drops    : 43321
Dell#
```

Example (drop summary)

```
Dell#show hard stack-unit 0 drops unit 0

PortNumber Ingress Drops IngMac Drops Total Mmu Drops EgMac
Drops Egress Drops
1          0             0            0
0           0
2          0             0            0
0           0
3          0             0            0
0           0
4          0             0            0
0           0
Dell#
```

Example (drop counters)

```
Dell#show hardware stack-unit 0 drops unit 0 port 27
  --- Ingress Drops ---
Ingress Drops               : 0
IBP CBP Full Drops          : 0
PortSTPnotFwd Drops         : 0
IPv4 L3 Discards            : 0
Policy Discards             : 0
Packets dropped by FP       : 0
(L2+L3) Drops               : 0
Port bitmap zero Drops      : 0
Rx VLAN Drops               : 0
  --- Ingress MAC counters---
Ingress FCSDrops            : 0
Ingress MTUExceeds          : 0
  --- MMU Drops ---
HOL DROPS                   : 0
TxPurge CellErr             : 0
Aged Drops                  : 0
  --- Egress MAC counters---
Egress FCS Drops            : 0
  --- Egress FORWARD PROCESSOR Drops ---
IPv4 L3UC Aged & Drops      : 0
TTL Threshold Drops         : 0
INVALID VLAN CNTR Drops     : 0
```

```
L2MC Drops                    : 0
PKT Drops of ANY Conditions : 0
Hg MacUnderflow               : 0
TX Err PKT Counter            : 0 25
Dell#
```

Example (port-statistics)

```
Dell#show hardware stack-unit 0 unit 0 port-stats
     ena/  speed/ link auto  STP               lrn inter max
loop
port link  duplex scan neg?  state pause discrd ops face frame
back
 xe0 !ena  1G FD    SW Yes   Forward        Tag   F GMII  1550
 xe1 !ena  1G FD    SW Yes   Forward        Tag   F GMII  1554
 xe2 up    1G FD    SW Yes   Forward       None  FA GMII 11996
 xe3 !ena  1G FD    SW Yes   Forward        Tag   F GMII  1550
 xe4 down  10G FD   SW Yes     Block       None  FA   KR  8996
 xe5 !ena  1G FD    SW Yes   Forward        Tag   F GMII  1550
 xe6 !ena  1G FD    SW Yes   Forward        Tag   F GMII  1550
 xe7 !ena  1G FD    SW Yes   Forward        Tag   F GMII  1550
 xe8 !ena  1G FD    SW Yes   Forward        Tag   F GMII  1550
 xe9 !ena  1G FD    SW Yes   Forward        Tag   F GMII  1550
 xe10 down 10G FD   SW Yes   Forward        Tag   F   KR  1550
 xe11 !ena 1G FD    SW Yes   Forward        Tag   F GMII  1550
 xe12 !ena 1G FD    SW Yes     Block       None  FA GMII 11996
 xe13 !ena 1G FD    SW Yes   Forward        Tag   F GMII  1550
 xe14 !ena 1G FD    SW Yes   Forward        Tag   F GMII  1550
 xe15 !ena 1G FD    SW Yes   Forward        Tag   F GMII  1550
 xe16 !ena 1G FD    SW Yes   Forward        Tag   F GMII  1550
 xe17 !ena 1G FD    SW Yes   Forward        Tag   F GMII  1550
 xe18 down 1G FD    SW Yes   Forward        Tag   F GMII  1550
 xe19 !ena 1G FD    SW Yes   Forward        Tag   F GMII  1550
 xe20 down 1G FD    SW Yes   Forward        Tag   F GMII  1550
Dell#
```

Example (register)

```
Dell#show hardware stack-unit 0 unit 0 register
0x0f180d34 ALTERNATE_EMIRROR_BITMAP_PARITY_CONTROL.ipipe0 =
0x00000001
0x0f180d35 ALTERNATE_EMIRROR_BITMAP_PARITY_STATUS_INTR.ipipe0
= 0x00000000
0x0f180d36 ALTERNATE_EMIRROR_BITMAP_PARITY_STATUS_NACK.ipipe0
= 0x00000000
0x0018070c ARB_EOP_DEBUG.ipipe0 = 0x00000000
0x00180312 ARB_RAM_DBGCTRL.ipipe0 = 0x00000000
0x03300000 ASF_PORT_SPEED.cpu0 = 0x00000000
0x03322000 ASF_PORT_SPEED.xe0 = 0x00000000
0x03326000 ASF_PORT_SPEED.xe1 = 0x00000000
0x0332a000 ASF_PORT_SPEED.xe2 = 0x00000007
0x0332e000 ASF_PORT_SPEED.xe3 = 0x00000000
0x03323000 ASF_PORT_SPEED.xe4 = 0x00000000
0x03327000 ASF_PORT_SPEED.xe5 = 0x00000000
0x0332b000 ASF_PORT_SPEED.xe6 = 0x00000000
0x0332f000 ASF_PORT_SPEED.xe7 = 0x00000000
0x03324000 ASF_PORT_SPEED.xe8 = 0x00000000
0x03328000 ASF_PORT_SPEED.xe9 = 0x00000000
0x0332c000 ASF_PORT_SPEED.xe10 = 0x00000000
0x03330000 ASF_PORT_SPEED.xe11 = 0x00000000
0x03325000 ASF_PORT_SPEED.xe12 = 0x00000000
0x03329000 ASF_PORT_SPEED.xe13 = 0x00000000
0x0332d000 ASF_PORT_SPEED.xe14 = 0x00000000
0x03331000 ASF_PORT_SPEED.xe15 = 0x00000000
0x03332000 ASF_PORT_SPEED.xe16 = 0x00000000
0x03336000 ASF_PORT_SPEED.xe17 = 0x00000000
```

```
0x0333a000 ASF_PORT_SPEED.xe18 = 0x00000000
0x0333e000 ASF_PORT_SPEED.xe19 = 0x00000000
0x03333000 ASF_PORT_SPEED.xe20 = 0x00000000
0x03337000 ASF_PORT_SPEED.xe21 = 0x00000000
0x0333b000 ASF_PORT_SPEED.xe22 = 0x00000000
0x0333f000 ASF_PORT_SPEED.xe23 = 0x00000000
0x03334000 ASF_PORT_SPEED.xe24 = 0x00000000
0x03338000 ASF_PORT_SPEED.xe25 = 0x00000000
0x0333c000 ASF_PORT_SPEED.xe26 = 0x00000000
0x03340000 ASF_PORT_SPEED.xe27 = 0x00000000
0x03335000 ASF_PORT_SPEED.xe28 = 0x00000000
0x03339000 ASF_PORT_SPEED.xe29 = 0x00000000
!----------------- output truncated ---------------!
```

Example (unit details)

```
Dell#show hardware stack-unit 0 unit 0 details

*****************************************************

The total no of FP & CSF Devices in the Card is 1
The total no of FP Devices in the Card is 1
The total no of CSF Devices in the Card is 0
The number of ports in device 0 is - 49
The number of Hg ports in devices 0 is - 1
The CPU Port of the device is 0
The staring unit no the SWF in the device is 0
*****************************************************

bcmLinkMonStatusShow: The Current Link Status Is

Front End Link Status         0x2000000000000000000000000
Front End Port Present Status 0x0000000000000000000000000
Back Plane Link Status        0x00000000

*****************************************************

Link Status of all the ports in the Device - 0

The linkStatus of Front End Port 1 is FALSE
The linkStatus of Front End Port 2 is FALSE
The linkStatus of Front End Port 3 is TRUE
The linkStatus of Front End Port 4 is FALSE
The linkStatus of Front End Port 5 is FALSE
The linkStatus of Front End Port 6 is FALSE
The linkStatus of Front End Port 7 is FALSE
The linkStatus of Front End Port 8 is FALSE
The linkStatus of Front End Port 9 is FALSE
The linkStatus of Front End Port 10 is FALSE
The linkStatus of Front End Port 11 is FALSE
The linkStatus of Front End Port 12 is FALSE
The linkStatus of Front End Port 13 is FALSE
The linkStatus of Front End Port 14 is FALSE
The linkStatus of Front End Port 15 is FALSE
The linkStatus of Front End Port 16 is FALSE
The linkStatus of Front End Port 17 is FALSE
The linkStatus of Front End Port 18 is FALSE
The linkStatus of Front End Port 19 is FALSE
The linkStatus of Front End Port 20 is FALSE
The linkStatus of Front End Port 21 is FALSE
The linkStatus of Front End Port 22 is FALSE
The linkStatus of Front End Port 23 is FALSE
The linkStatus of Front End Port 24 is FALSE
The linkStatus of Front End Port 25 is FALSE
The linkStatus of Front End Port 26 is FALSE
The linkStatus of Front End Port 27 is FALSE
The linkStatus of Front End Port 28 is FALSE
The linkStatus of Front End Port 29 is FALSE
The linkStatus of Front End Port 30 is FALSE
The linkStatus of Front End Port 31 is FALSE
The linkStatus of Front End Port 32 is FALSE
The linkStatus of Front End Port 37 is FALSE
!------------------ output truncated ---------------!
```

Example (buffer)

```
Dell(conf)#sh hardware stack-unit 0 buffer total-buffer

Dell#sh hardware stack-unit 0 buffer total-buffer

Total Buffers allocated per Stack-Unit 46080
```

Example (specific port)

```
Dell(conf)#show hardware stack-unit 0 buffer unit 0 port 1
buffer-info
-----  Buffer Stats for Unit 0 Port 1 -----
Maximum Shared Limit for the Port: 30720
Default Packet Buffer allocate for the Port: 120

Used Packet Buffer for the Port: 0
```

Example (queue buffer)

```
Dell(conf)#show hardware stack-unit 0 buffer unit 0 port 1
queue 2 buffer-info

----- Buffer Stats for Unit 0 Port 1 Queue 2 -----
  Maximum Shared Limit: 30720
  Default Packet Buffer allocate for the Queue: 8
  Used Packet Buffer: 0
```

Related Commands

clear hardware system-flow — clears the statistics from selected hardware components.

show interfaces stack-unit — displays information on all interfaces on a specific stack member.

show processes cpu — Displays CPU usage information based on running processes.

show system stack-ports — Displays information about the stacking ports on all switches in the stack.

show system — Displays the current status of all stack members or a specific member.

show hardware system-flow

Display Layer 3 ACL or QoS data for the selected stack member and stack member port-pipe.

Syntax

```
show hardware system-flow layer2 stack-unit 0-5 port-set 0-0
[counters]
```

Parameters

acl | qos	For the selected stack member and stack member port-pipe, display which system flow entry the packet hits and what queue the packet takes as it dumps the raw system flow tables.
stack-unit *0–5*	Enter the keywords `stack-unit` then 0 to 5 to select a stack member ID.
port-set *0–0* [counters]	Enter the keywords `port-set` with a port-pipe number. (OPTIONAL) Enter the keyword `counters` to display hit counters for the selected ACL or QoS option.

Defaults none

Command Modes EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show hardware system-flow layer2 stack-unit 0 port-set 0
counters
---------------------------------------------------------------
EntryId  Description                 #HITS
---------------------------------------------------------------
2048     STP BPDU Redirects           0
2047     LLDP BPDU Redirects          164904
2045     LACP traffic Redirects       0
2044     GVRP traffic Redirects       0
2043     ARP Reply Redirects          0
2042     802.1x frames Redirects      0
2041     VRRP frames Redirects        0
2040     IPv6VRRP frames Redirects    0
2039     GRAT ARP                     0
2036     IPv6 Mcast Control Traffic   128840
2000     VLT ARP SYNC Frames          0
1999     ICL Hellos                   0
1998     ICL MAC SYNC Frames          0
1997     VLT Tunneled STP Frames      0
1995     DROP Cases                   43207
1917     L3 Term Traffic ClassID 1 to Q6       0
1916     L3 CPU Bound Traffic ClassId 2 to Q5  0
1915     Unknown MCAST Packets                 0
1792     BGP with TTL1, L4 SRC port Redirects  0
1791     BGP with TTL1, L4 DST Port Redirects  0
25
Dell#
```

Example (non-counters)

```
Dell#show hardware system-flow layer2 stack-unit 0 port-set 0

############## FP Entry for redirecting STP BPDU to CPU Port
################
EID 2048: gid=1,
    slice=15, slice_idx=0x00, prio=0x800, flags=0x82, Installed
        tcam: color_indep=0, higig=0, higig_mask=0,
        KEY=0x00000000 00000000 00000000 0180c200 00000000
00000000 00000000
```

```
, FPF4=0x00
        MASK=0x00000000 00000000 00000000 ffffffff ffff0000
00000000 00000000
,       0x00
          action={act=Drop, param0=0(0x00), param1=0(0x00)},
          action={act=CosQCpuNew, param0=7(0x07),
param1=0(0x00)},
          action={act=CopyToCpu, param0=0(0x00),
param1=0(0x00)},
          action={act=UpdateCounter, param0=1(0x01),
param1=0(0x00)},
          meter=NULL,
          counter={idx=0, mode=0x01, entries=1}

################ FP Entry for redirecting LLDP BPDU to RSM
################
EID 2047: gid=1,
          slice=15, slice_idx=0x01, prio=0x7ff, flags=0x82,
Installed
             tcam: color_indep=0, higig=0, higig_mask=0,
             KEY=0x00000000 00000000 00000000 0180c200
000e0000 00000000 00000000
, FPF4=0x00
          MASK=0x00000000 00000000 00000000 ffffffff ffff0000
00000000 00000000
,      0x00
action={act=Drop, param0=0(0x00), param1=0(0x00)},
          action={act=CosQCpuNew, param0=7(0x07),
param1=0(0x00)},
          action={act=CopyToCpu, param0=0(0x00),
param1=0(0x00)},
          action={act=UpdateCounter, param0=1(0x01),
param1=0(0x00)},
          meter=NULL,
          counter={idx=1, mode=0x01, entries=1}

############## FP Entry for redirecting LACP traffic to CPU
Port ############
EID 2045: gid=1,
          slice=15, slice_idx=0x02, prio=0x7fd, flags=0x82,
Installed
            tcam: color_indep=0, higig=0, higig_mask=0,
           KEY=0x00000000 00000000 00000000 0180c200 00020000
00000000 00000000
, FPF4=0x00
           MASK=0x00000000 00000000 00000000 ffffffff ffff0000
00000000 00000000
,      0x00
          action={act=Drop, param0=0(0x00), param1=0(0x00)},
          action={act=CosQCpuNew, param0=7(0x07),
param1=0(0x00)},
          action={act=CopyToCpu, param0=0(0x00),
param1=0(0x00)},
          action={act=UpdateCounter, param0=1(0x01),
param1=0(0x00)},
          meter=NULL,
          counter={idx=2, mode=0x01, entries=1}

################# FP Entry for redirecting GVRP traffic to RSM
###########
EID 2044: gid=1,
         slice=15, slice_idx=0x03, prio=0x7fc, flags=0x82,
Installed
           tcam: color_indep=0, higig=0, higig_mask=0,
           KEY=0x00000000 00000000 00000000 0180c200 00210000
00000000 00000000
, FPF4=0x00
           MASK=0x00000000 00000000 00000000 ffffffff ffff0000
00000000 00000000
,      0x00
           action={act=Drop, param0=0(0x00), param1=0(0x00)},
           action={act=CosQCpuNew, param0=7(0x07),
param1=0(0x00)},
           action={act=CopyToCpu, param0=0(0x00),
param1=0(0x00)},
           action={act=UpdateCounter, param0=1(0x01),
param1=0(0x00)},
           meter=NULL,
           counter={idx=3, mode=0x01, entries=1}

################# FP Entry for redirecting ARP Replies to RSM
#############
EID 2043: gid=1,
           slice=15, slice_idx=0x04, prio=0x7fb, flags=0x82,
Installed
             tcam: color_indep=0, higig=0, higig_mask=0,
             KEY=0x00000000 00000000 00000000 00000000
00000000 00000806 00001600
, FPF4=0x00
             MASK=0x00000000 00000000 00000000 00000000
00000000 0000ffff 00001600
,      0x00
           action={act=Drop, param0=0(0x00), param1=0(0x00)},
           action={act=CosQCpuNew, param0=6(0x06),
param1=0(0x00)},
           action={act=CopyToCpu, param0=0(0x00),
param1=0(0x00)},
           action={act=UpdateCounter, param0=1(0x01),
param1=0(0x00)},
!--------- output truncated -----------------!
```

14

Dynamic Host Configuration Protocol (DHCP)

Dynamic host configuration protocol (DHCP) is an application layer protocol that dynamically assigns IP addresses and other configuration parameters to network end-stations (hosts) based on the configuration policies the network administrators determine.

An MXL switch can operate as a DHCP server or DHCP client. As a DHCP client, the switch requests an IP address from a DHCP server.

This chapter contains the following sections:

- Commands to Configure the System to be a DHCP Client
- Commands to Configure the System to be a DHCP Server
- Commands to Configure Secure DHCP

Commands to Configure the System to be a DHCP Server

To configure the system to be a DHCP server, use the following commands.

clear ip dhcp

Reset the DHCP counters.

Syntax

```
clear ip dhcp [binding {address} | conflict | server
statistics]
```

Parameters

binding	Enter the keyword `binding` to delete all entries in the binding table.
address	Enter the IP address to clear the binding entry for a single IP address.
conflicts	Enter the keyword `conflicts` to delete all of the log entries created for IP address conflicts.
server statistics	Enter the keywords `server statistics` to clear all the server counter information.

Defaults none

Command Modes	EXEC Privilege
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	Entering <CR> after the `clear ip dhcp binding` command clears all the IPs from the binding table.

debug ip dhcp server

Display the Dell Networking OS debugging messages for DHCP.

Syntax	`debug ip dhcp server [events | packets]`	
Parameters	**events**	Enter the keyword `events` to display the DHCP state changes.
	packet	Enter the keyword `packet` to display packet transmission/ reception.
Defaults	none	
Command Modes	EXEC Privilege	
Command History	**Version 8.3.16.1**	Introduced on the MXL 10/40GbE Switch IO Module.

default-router

Assign a default gateway to clients based on the address pool.

Syntax	`default-router` *`address`* `[`*`address2...address8`*`]`	
Parameters	***address***	Enter a list of routers that may be the default gateway for clients on the subnet. You may specify up to eight routers. List them in order of preference.
Defaults	none	
Command Modes	DHCP <POOL>	
Command History	**Version 8.3.16.1**	Introduced on the MXL 10/40GbE Switch IO Module.

disable

Disable the DHCP server.

Syntax `disable`

DHCP Server is disabled by default. To enable the system to be a DHCP server, use the `no disable` command.

Defaults Disabled

Command Modes DHCP

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

dns-server

Assign a DNS server to clients based on address pool.

Syntax `dns-server address [address2...address8]`

Parameters

address	Enter a list of DNS servers that may service clients on the subnet. You may list up to eight servers, in order of preference.

Defaults none

Command Modes DHCP <POOL>

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

domain-name

Assign a domain to clients based on the address pool.

Syntax `domain-name` *`name`*

Parameters

name	Give a name to the group of addresses in a pool.

Defaults none

Command Modes DHCP <POOL>

Command History	**Version 8.3.16.1**	Introduced on the MXL 10/40GbE Switch IO Module.

excluded-address

Prevent the server from leasing an address or range of addresses in the pool.

Syntax `excluded-address [address | low-address high-address]`

Parameters

address	Enter a single address to be excluded from the pool.
low-address	Enter the lowest address in a range of addresses to be excluded from the pool.
high-address	Enter the highest address in a range of addresses to be excluded from the pool.

Defaults none

Command Modes DHCP

Command History	**Version 8.3.16.1**	Introduced on the MXL 10/40GbE Switch IO Module.

hardware-address

For manual configurations, specify the client hardware address.

Syntax `hardware-address address`

Parameters

address	Enter the hardware address of the client.

Defaults none

Command Modes DHCP <POOL>

Command History	**Version 8.3.16.1**	Introduced on the MXL 10/40GbE Switch IO Module.

host

For manual (rather than automatic) configurations, assign a host to a single-address pool.

Syntax `host address`

Parameters

address/mask	Enter the host IP address and subnet mask.

Defaults none

Command Modes DHCP <POOL>

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

lease

Specify a lease time for the addresses in a pool.

Syntax `lease {days [hours] [minutes] | infinite}`

Parameters

days	Enter the number of days of the lease. The range is from 0 to 31.
hours	Enter the number of hours of the lease. The range is from 0 to 23.
minutes	Enter the number of minutes of the lease. The range is from 0 to 59.
infinite	Specify that the lease never expires.

Defaults **24 hours**

Command Modes DHCP <POOL>

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

netbios-name-server

Specify the NetBIOS windows internet naming service (WINS) name servers, in order of preference, that are available to Microsoft dynamic host configuration protocol (DHCP) clients.

Syntax `netbios-name-server address [address2...address8]`

Parameters	*address*	Enter the address of the NETBIOS name server. You may enter up to eight, in order of preference.
Defaults	none	
Command Modes	DHCP <POOL>	
Command History	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

netbios-node-type

Specify the NetBIOS node type for a Microsoft DHCP client. Dell Networking Operating System (OS) recommends specifying clients as `hybrid`.

Syntax	`netbios-node-type` *`type`*	
Parameters	*type*	Enter the NETBIOS node type: • Broadcast: Enter the keyword `b-node`. • Hybrid: Enter the keyword `h-node`. • Mixed: Enter the keyword `m-node`. • Peer-to-peer: Enter the keyword `p-node`.
Defaults	**Hybrid**	
Command Modes	DHCP <POOL>	
Command History	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

network

Specify the range of addresses in an address pool.

Syntax	`network` *`network /prefix-length`*	
Parameters	*network/ prefix-length*	Specify a range of addresses. Prefix-length range is from 17 to 31.
Defaults	none	

Command Modes	DHCP <POOL>
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

show ip dhcp binding

Display the DHCP binding table.

Syntax	`show ip dhcp binding`
Defaults	none
Command Modes	EXEC Privilege
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

show ip dhcp configuration

Display the DHCP configuration.

Syntax `show ip dhcp configuration [global | pool name]`

Parameters

pool *name*	Display the configuration for a DHCP pool.
global	Display the DHCP configuration for the entire system.

Defaults	none
Command Modes	EXEC Privilege
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

show ip dhcp conflict

Display the address conflict log.

Syntax `show ip dhcp conflict address`

Parameters

address	Display a particular conflict log entry.

Defaults	none
Command Modes	EXEC Privilege
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

show ip dhcp server

Display the DHCP server statistics.

Syntax	`show ip dhcp server statistics`
Defaults	none
Command Modes	EXEC Privilege
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

Commands to Configure the System to be a DHCP Client

To configure the system to be a DHCP client, use the following commands.

ip address dhcp

Configure an Ethernet interface to acquire its IP address from a DHCP network server.

Syntax	`ip address dhcp`
Command Modes	INTERFACE
Default	The Ethernet is not configured to operate as a DHCP client and receive a dynamic IP address.
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	The `ip address dhcp` command enables an Ethernet interface to acquire a DHCP server-assigned dynamic IP address. This setting persists after a switch reboot. If you enter the `shutdown` command on the interface, DHCP transactions are stopped and the dynamically-acquired IP address is saved. To display the dynamic IP address and DHCP as the mode of IP address assignment, use the `show`

`interface type slot/port` command. If you later enter the `no shutdown]` command and the lease timer for the dynamic IP address has expired, the IP address is unconfigured and the interface tries to acquire a new dynamic address from DHCP server.

You cannot configure a secondary (backup) IP address on an interface using the `ip address dhcp` command; you must use the `ip address` command at the interface configuration level.

To release a DHCP-assigned IP address and remove the interface from being a DHCP client, use the `no ip address dhcp` command. When you use the `no ip address dhcp` command:

- The IP address dynamically acquired from a DHCP server is released from the interface.
- The DHCP client is disabled on the interface; it can no longer acquire a dynamic IP address from a DHCP server.
- DHCP packet transactions on the interface are stopped.

To display the currently configure dynamic IP address and lease time, use the `show ip dhcp lease` command.

Other Commands Supported by the DHCP Client

The following commands are supported by the DHCP client.

clear ip dhcp client statistics

Display DHCP client statistics, including the number of DHCP messages sent and received on an interface.

Syntax

```
clear ip dhcp client statistics {all | interface type slot/
port}
```

Parameters

all	Clear DHCP client statistics on all DHCP client-enabled interfaces on the switch.
interface type *slot/ port*	Clear DHCP client statistics on the specified interface. • For a 10-GigabitEthernet Ethernet interface, enter `TenGigabitEthernet` then the slot/port numbers; for example, `tengigabitethernet 1/3`. • For a 40-GigabitEthernet Ethernet interface, enter `FortyGigabitEthernet` then the slot/port numbers; for example, `fortygigabitethernet 0/2`.

Defaults none

Command Modes EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

debug ip dhcp clients events

Enable the display of log messages for the following events on DHCP client interfaces: IP address acquisition, IP address release, Renewal of IP address and lease time, and Release of an IP address.

Syntax `debug ip dhcp client events [interface type slot/port]`

Parameters

interface type *slot/ port*	Display log messages for DHCP events on the specified interface. - For a 10-GigabitEthernet Ethernet interface, enter `TenGigabitEthernet` then the slot/port numbers; for example, `tengigabitethernet 1/3`. - For a 40-GigabitEthernet Ethernet interface, enter `FortyGigabitEthernet` then the slot/port numbers; for example, `fortygigabitethernet 0/2`.

Defaults none

Command Modes EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

debug ip dhcp clients packets

Enable the display of log messages for all DHCP packets sent and received on DHCP client interfaces.

Syntax `debug ip dhcp client packets [interface type slot/port]`

Parameters

interface *type slot/ port*	Display log messages for DHCP packets sent and received on the specified interface. - For a 10-GigabitEthernet Ethernet interface, enter `TenGigabitEthernet` then the slot/port numbers; for example, `tengigabitethernet 1/3`. - For a 40-GigabitEthernet Ethernet interface, enter `FortyGigabitEthernet` then the slot/port numbers; for example, `fortygigabitethernet 0/2`.

Defaults	none
Command Modes	EXEC Privilege
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

release dhcp interface

Release the dynamically-acquired IP address on an Ethernet interface while retaining the DHCP client configuration on the interface.

Syntax `release dhcp interface` *`type slot/port`*

Parameters

interface *type slot/port*	• For a 10-GigabitEthernet Ethernet interface, enter `TenGigabitEthernet` then the slot/port numbers; for example, `tengigabitethernet 1/3`. • For a 40-GigabitEthernet Ethernet interface, enter `FortyGigabitEthernet` then the slot/port numbers; for example, `fortygigabitethernet 0/2`.

Defaults	none
Command Modes	EXEC Privilege
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	When you enter the `release dhcp` command, although the IP address that was dynamically-acquired from a DHCP server is released from an interface, the ability to acquire a new DHCP server-assigned address remains in the running configuration for the interface. To acquire a new IP address, enter either the `renew dhcp` command at the EXEC privilege level or the `ip address dhcp` command at the Interface Configuration level.

renew dhcp interface

Re-acquire a dynamic IP address on an Ethernet interface enabled as a DHCP client.

Syntax `renew dhcp interface` *`type slot/port`*

Parameters

interface *type slot/port*	• For a 10-GigabitEthernet Ethernet interface, enter `TenGigabitEthernet` then the slot/port numbers; for example, `tengigabitethernet 1/3`.

- For a 40-GigabitEthernet Ethernet interface, enter `FortyGigabitEthernet` then the slot/port numbers; for example, `fortygigabitethernet 0/2`.

Defaults none

Command Modes EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

When you enter the `renew dhcp` command, a new dynamic IP address is acquired on the specified Ethernet interface for the renewed lease time.

To display the currently configure dynamic IP address and lease time, enter the `show ip dhcp lease` command.

show ip dhcp client statistics

Display DHCP client statistics, including the number of DHCP messages sent and received on an interface.

Syntax `show ip dhcp client statistics {all | interface type slot/port}`

Parameters

all	Display DHCP client statistics on all DHCP client-enabled interfaces on the switch.
interface *type slot/port*	Display DHCP client statistics on the specified interface. • For a 10-GigabitEthernet Ethernet interface, enter `TenGigabitEthernet` then the slot/port numbers; for example, `tengigabitethernet 1/3`. • For a 40-GigabitEthernet Ethernet interface, enter `FortyGigabitEthernet` then the slot/port numbers; for example, `fortygigabitethernet 0/2`.

Defaults none

Command Modes EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

show ip dhcp lease

Display lease information about the dynamic IP address currently assigned to a DHCP client-enabled interface.

Syntax	`show ip dhcp lease [interface type slot/port]`
Parameters	

interface *type slot/port*	Display DHCP lease information on the specified interface. • For a 10-GigabitEthernet Ethernet interface, enter `TenGigabitEthernet` then the slot/port numbers; for example, `tengigabitethernet 1/3`. • For a 40-GigabitEthernet Ethernet interface, enter `FortyGigabitEthernet` then the slot/port numbers; for example, `fortygigabitethernet 0/2`.

Defaults	Display DHCP lease information on all DHCP client-enabled interfaces on the switch.
Command Modes	EXEC Privilege
Command History	

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Commands to Configure Secure DHCP

DHCP, as defined by RFC 2131, provides no authentication or security mechanisms. Secure DHCP is a suite of features that protects networks that use dynamic address allocation from spoofing and attacks.

arp inspection

Enable dynamic arp inspection (DAI) on a VLAN.

Syntax	`arp inspection`
Defaults	Disabled
Command Modes	INTERFACE VLAN
Command History	

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands	arp inspection-trust — specifies a port as trusted so that ARP frames are not validated against the binding table.

arp inspection-trust

Specify a port as trusted so that ARP frames are not validated against the binding table.

Syntax	`arp inspection-trust`
Defaults	Disabled
Command Modes	- INTERFACE - INTERFACE PORT-CHANNEL
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	arp inspection — enables dynamic ARP inspection on a VLAN.

clear ip dhcp snooping

Clear the DHCP binding table.

Syntax	`clear ip dhcp snooping binding`
Defaults	none
Command Modes	EXEC Privilege
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	show ip dhcp snooping — displays the contents of the DHCP binding table.

ip dhcp snooping

Enable DHCP snooping globally.

Syntax	`[no] ip dhcp snooping`
Defaults	Disabled
Command Modes	CONFIGURATION
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information	When enabled, no learning takes place until you enable snooping on a VLAN. After disabling DHCP snooping, the binding table is deleted, and Option 82, IP Source Guard, and Dynamic ARP Inspection are disabled. Introduced in the Dell Networking OS version 7.8.1.0, DHCP snooping was available for Layer 3 only and dependent on DHCP Relay Agent (ip helper-address). The Dell Networking OS version 8.2.1.0 extends DHCP Snooping to Layer 2, and you do not have to enable relay agent to snoop on Layer 2 interfaces.
Related Commands	ip dhcp snooping vlan — enables DHCP snooping on one or more VLANs.

ip dhcp snooping database

Delay writing the binding table for a specified time.

Syntax	`ip dhcp snooping database write-delay` *`minutes`*
Parameters	*minutes* — The range is from 5 to 21600.
Defaults	none
Command Modes	CONFIGURATION
Command History	Version 8.3.16.1 — Introduced on the MXL 10/40GbE Switch IO Module.

ip dhcp snooping binding

Create a static entry in the DHCP binding table.

Syntax	`[no] ip dhcp snooping binding mac` *`address`* `vlan-id` *`vlan-id`* `ip` *`ip-address`* `interface` *`type slot/port`* `lease` *`number`*

Parameters

mac *address*	Enter the keyword `mac` then the MAC address of the host to which the server is leasing the IP address.
vlan-id *vlan-id*	Enter the keywords `vlan-id` then the VLAN to which the host belongs. The range is from 2 to 4094.
ip *ip-address*	Enter the keyword `ip` then the IP address that the server is leasing.
interface *type*	Enter the keyword `interface` then the type of interface to which the host is connected:

	- For a Ten-Gigabit Ethernet interface, enter the keyword `tengigabitethernet`. - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE`.
slot/port	Enter the slot and port number of the interface.
lease *time*	Enter the keyword `lease` then the amount of time the IP address are leased. The range is from 1 to 4294967295.

Defaults	none
Command Modes	- EXEC - EXEC Privilege
Command History	Version 8.3.16.1 — Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	show ip dhcp snooping — displays the contents of the DHCP binding table.

ip dhcp snooping database renew

Renew the binding table.

Syntax	`ip dhcp snooping database renew`
Defaults	none
Command Modes	- EXEC - EXEC Privilege
Command History	Version 8.3.16.1 — Introduced on the MXL 10/40GbE Switch IO Module.

ip dhcp snooping trust

Configure an interface as trusted.

Syntax	`[no] ip dhcp snooping trust`
Defaults	**Untrusted**
Command Modes	INTERFACE

Command History	**Version 8.3.16.1**	Introduced on the MXL 10/40GbE Switch IO Module.

ip dhcp source-address-validation

Enable the IP Source Guard.

Syntax `[no] ip dhcp source-address-validation [ipmac]`

Parameters

ipmac	Enable IP+MAC Source Address Validation.

Defaults Disabled

Command Modes INTERFACE

Command History	**Version 8.3.16.1**	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Allocate at least one FP block to `ipmacacl` before you can enable IP+MAC Source Address Validation.

1. Use the `cam-acl l2acl` command from CONFIGURATION mode.
2. Save the running-config to the startup-config.
3. Reload the system.

ip dhcp snooping vlan

Enable DHCP Snooping on one or more VLANs.

Syntax `[no] ip dhcp snooping vlan` *`name`*

Parameters

name	Enter the name of a VLAN on which to enable DHCP Snooping.

Defaults Disabled

Command Modes CONFIGURATION

Command History	**Version 8.3.16.1**	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

When enabled, the system begins creating entries in the binding table for the specified VLANs.

NOTE: Learning only happens if there is a trusted port in the VLAN.

Related Commands	ip dhcp snooping trust — configures an interface as trusted.

ip dhcp relay

Enable Option 82.

Syntax `ip dhcp relay information-option [remote-id | trust-downstream]`

Parameters

remote-id	Configure the system to enable the remote-id string in option-82.
trust-downstream	Configure the system to trust Option 82 when it is received from the previous-hop router.

Defaults Disabled

Command Modes CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

show ip dhcp snooping

Display the contents of the DHCP binding table or display the interfaces configured with IP Source Guard.

Syntax `show ip dhcp snooping [binding | source-address-validation]`

Parameters

binding	Display the interfaces configured with IP Source Guard.
source-address-validation	Display the interfaces configured with IP Source Guard.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands	clear ip dhcp snooping — clears the contents of the DHCP binding table.

ip dhcp snooping verify mac-address

Validate a DHCP packet's source hardware address against the client hardware address field (CHADDR) in the payload.

Syntax	`[no] ip dhcp snooping verify mac-address`
Defaults	Disabled
Command Modes	CONFIGURATION
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

15

Equal Cost Multi-Path (ECMP)

Equal cost multi-path (ECMP) is supported on the Dell Networking MXL 10/40GbE Switch IO Module.

ecmp-group

Provides a mechanism to monitor traffic distribution on an ECMP link bundle. A system log is generated when the standard deviation of traffic distribution on a member link exceeds a defined threshold.

Syntax

`ecmp-group {ecmp-group-id interface interface | link-bundle-monitor}`

To remove the selected interface, use the `ecmp-group no interface` command.

To disable link bundle monitoring, use the `ecmp-group no link-bundle-monitor` command.

Parameters

ecmp-group ID	Enter the identifier number for the ECMP group. The range is from 2 to 64.
interface	Enter the following keywords and slot/port to add the interface to the ECMP group: • 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information
link-bundle-monitor	Enter the keywords `link-bundle-monitor` to enable link bundle monitoring.

Defaults

Off

Command Modes

- CONFIGURATION
- CONFIGURATION ECMP-GROUP

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

hash-algorithm

Changes the hash algorithm used to distribute traffic flows across a Port Channel.

Syntax

```
hash-algorithm {algorithm-number | {ecmp {crc16 | crc16cc |
crc32MSB | crc32LSB | crc-upper | dest-ip | lsb | xor1 | xor2 |
xor4 | xor8 | xor16} [number] lag {checksum | crc | xor}
[number] nh-ecmp {checksum | crc | xor}[number] linecard number
ip-sa-mask value ip-da-mask value | seed seed-value }
```

To return to the default hash algorithm, use the `no hash-algorithm` command.

To return to the default ECMP hash algorithm, use the `no hash-algorithm ecmp algorithm-value` command.

To remove the hash algorithm on a particular line card, use the `no hash-algorithm linecard number` command.

Parameters

algorithm-number	Enter the algorithm number. The range is from 0 to 47.
ecmp {*crc16* | *crc16cc* | *crc32MSB* | *crc32LSB* | *crc-upper* | *dest-ip* | *lsb* | *xor1* | *xor2* | *xor4* | *xor8* | *xor16*}	TeraScale and ExaScale Only: Enter the keyword `ecmp` then one of the following options: • *crc16*: Use CRC16_BISYNC — 16 bit CRC16-bisync polynomial (default) • *crc16cc*: Use CRC16_CCITT — 16 bit CRC16 using CRC16-CCITT polynomial • *crc32MSB*: Use CRC32_UPPER — MSB 16 bits of computed CRC32 • *crc32LSB*: Use CRC32_LOWER — LSB 16 bits of computed CRC32 • *crc-upper*: Uses the upper 32 bits of the key for the hash computation • *dest-ip*: Uses the destination IP for ECMP hashing • *lsb*: Returns the LSB of the key as the hash • *xor1*: Use CRC16_BISYNC_AND_XOR1 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor1 • *xor2*: Use CRC16_BISYNC_AND_XOR2 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor2 • *xor4*: Use CRC16_BISYNC_AND_XOR4 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor4 • *xor8*: Use CRC16_BISYNC_AND_XOR8 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor8 • *xor16*: Use CR16 — 16 bit XOR
lag hash *algorithm value*	Enter the keyword `lag` then the LAG hash algorithm value. The range is from 0 to 47.
nh-ecmp *hash algorithm value*	(OPTIONAL) Enter the keyword `nh-ecmp` then the ECMP hash algorithm value.

linecard *number*	(OPTIONAL) Enter the keyword `linecard` then the linecard slot number.
ip-sa-mask *value*	(OPTIONAL) Enter the keywords `ip-sa-mask` then the ECMP/LAG hash mask value. The range is from 0 to FF. The default is **FF**.
ip-da-mask *value*	(OPTIONAL) Enter the keywords `ip-da-mask` then the ECMP/LAG hash mask value. The range is from 0 to FF. The default is **FF**.

Defaults

0 for hash-algorithm value on TeraScale and ExaScale IPSA and IPDA mask value is **FF** for a line card.

Command Modes

CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To ensure that CRC is not used for LAG, set the default hash-algorithm method on ExaScale systems. For example,`hash-algorithm ecmp xor lag checksum nh-ecmp checksum.`

To achieve the functionality of hash-align on the ExaScale platform, do not use CRC as a hash-algorithm method.

The hash value calculated with the `hash-algorithm` command is unique to the entire chassis. The hash algorithm command with the line card option changes the hash for a particular line card by applying the mask specified in the IPSA and IPDA fields.

The line card option is applicable with the lag-hash-align microcode only (refer to CAM Profile Commands). Any other microcode returns an error message as follows:

- `Dell(conf)#hash-algorithm linecard 5 ip-sa-mask ff ip-da-mask ff`
- `% Error: This command is not supported in the current microcode configuration`

In addition, the `linecard` *`number`* `ip-sa-mask` *`value`* `ip-da-mask` *`value`* option has the following behavior to maintain bi-directionality:

- When hashing is done on both IPSA and IPDA, the `ip-sa-mask` and `ip-da-mask` values must be equal. (Single Linecard).
- When hashing is done only on IPSA or IPDA, the Dell Networking OS maintains bi-directionality with masks set to XX 00 for line card 1 and 00 XX for line card 2 (`ip-sa-mask` and `ip-da-mask`). The mask value must be the same for both line cards when using multiple line cards as ingress (where XX is any value from 00 to FF for both line cards). For example, assume that traffic is flowing between linecard 1 and linecard 2:
- `hash-algorithm linecard 1 ip-sa-mask aa ip-da-mask 00`

- `hash-algorithm linecard 2 ip-sa-mask 00 ip-da-mask aa`

The different hash algorithms are based on the number of Port Channel members and packet values. The default hash algorithm (number 0) yields the most balanced results in various test scenarios, but if the default algorithm does not provide a satisfactory distribution of traffic, use the hash-algorithm command to designate another algorithm.

When a Port Channel member leaves or is added to the Port Channel, the hash algorithm is recalculated to balance traffic across the members.

On TeraScale, if you do not enter the keyword `ECMP` or `LAG`, the Dell Networking OS assumes it to be common for both. If the keyword ECMP or LAG is entered separately, both should fall in the range of 0 to 23 or 24 to 47 since compression enable/disable is common for bothTeraScale and ExaScale support the range 0-47. The default for ExaScale is **24**.

hash-algorithm ecmp

Change the hash algorithm used to distribute traffic flows across an ECMP (equal-cost multipath routing) group.

Syntax

`hash-algorithm ecmp {crc-upper} | {dest-ip} | {lsb}`

To return to the default hash algorithm, use the `no hash-algorithm ecmp` command.

Parameters

crc-upper	Uses the upper 32 bits of the key for the hash computation. The default is **crc-lower**.
dest-ip	Uses the destination IP for ECMP hashing. The default is **enabled**.
lsb	Returns the LSB of the key as the hash. The default is **crc-lower**.

Defaults

- **crc-lower**
- **dest-ip enabled**

Command Modes

CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The hash value calculated with the `hash-algorithm` command is unique to the entire chassis. The default ECMP hash configuration is **crc-lower**. This command takes the lower 32 bits of the hash key to compute the egress port and is the “fall-back” configuration if you have not configured anything else.

The different hash algorithms are based on the number of ECMP group members and packet values. The default hash algorithm yields the most balanced results in various test scenarios, but if the default algorithm does not provide satisfactory distribution of traffic, use this command to designate another algorithm.

When a member leaves or is added to the ECMP group, the hash algorithm is recalculated to balance traffic across the members.

hash-algorithm seed

Select the seed value for the ECMP, LAG, and NH hashing algorithm.

Syntax `hash-algorithm seed value [linecard slot] [port-set number]`

Parameters

seed *value*	Enter the keyword `seed` then the seed value. The range is from 0 to 4095.
linecard *slot*	Enter the keyword `linecard` then the linecard slot number.
port-set *number*	Enter the keywords `port-set` then the linecard port-pipe number.

Defaults none

Command Modes CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Deterministic ECMP sorts ECMPs in order even though RTM provides them in a random order. However, the hash algorithm uses as a seed the lower 12 bits of the chassis MAC, which yields a different hash result for every chassis. This behavior means that for a given flow, even though the prefixes are sorted, two unrelated chassis select different hops.

The Dell Networking OS provides a CLI-based solution for modifying the hash seed to ensure that on each configured system, the ECMP selection is same. When configured, the same seed is set for ECMP, LAG, and NH, and is used for incoming traffic only.

NOTE: While the seed is stored separately on each port-pipe, the same seed is used across all CAMs.

You cannot separate LAG and ECMP but you can use different algorithms across the chassis with the same seed. If LAG member ports span multiple port-pipes and line cards, set the seed to the same value on each port-pipe to achieve deterministic behavior.

If the hash algorithm configuration is removed, the hash seed does not go to the original factory default setting.

ip ecmp-group

Enable and specify the maximum number of ecmp that the L3 CAM hold for a route, By default, when maximum paths are not configured, the CAM can hold a maximum of 16 ecmp per route.

Syntax

```
ip ecmp-group {maximum-paths | {number} {path-fallback}
```

To negate a command, use the `no ip ecmp-group maximum-paths` command.

Parameters

maximum-paths	Specify the maximum number of ECMP for a route. The range is 2 to 64.
path-fallback	Use the keywords `path-fallback` to enable this feature. If you enable the feature, re-enter this keyword to disable the feature.

Defaults

16

Command Modes

CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

You must save the new ECMP settings to the startup-config (`write-mem`) then reload the system for the new settings to take effect.

Related Commands

show ip cam stack-unit — Display content-addressable memory (CAM) entries.

link-bundle-distribution trigger-threshold

Provides a mechanism to set the threshold to trigger when traffic distribution begins being monitored on an ECMP link bundle.

Syntax

```
link-bundle-distribution trigger-threshold [percent]
```

Parameters	*percent*	Indicate the threshold value when traffic distribution starts being monitored on an ECMP link bundle. The range is from 1 to 90%. The default is **60%**.
Command Modes	EXEC Privilege	
Command History	Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

link-bundle-monitor enable

Provides a mechanism to enable monitoring of traffic distribution on an ECMP link bundle.

Syntax

```
link-bundle-monitor enable
```

To exit from ECMP group mode, use the `exit` command.

Command Modes

- ECMP-GROUP
- PORT-CHANNEL INTERFACE

Command History	Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

show config

Display the ECMP configuration.

Syntax

```
show config
```

Command Modes	CONFIGURATION-ECMP-GROUP	
Command History	Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

show link-bundle distribution

Display the link-bundle distribution for the interfaces in the bundle, type of bundle (LAG or ECMP), and the most recently calculated interface utilization (either bytes per second rate or maximum rate) for each interface.

Syntax	`show link-bundle-distribution`
Command Modes	EXEC Privilege
Command History	Version 9.2(0.0) — Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show link-bundle-distribution
Link-bundle trigger threshold - 60
ECMP bundle - 5 Utilization[In Percent] - 0 Alarm State -
Inactive
Interface Line Protocol Utilization[In Percent]
Te 0/4    Up            5
Te 0/3    Up            30
```

16

FIPS Cryptography

To configure federal information processing standards (FIPS) cryptography, use the following commands on the MXL 10/40GbE Switch IO Module.

fips mode enable

Enable the FIPS cryptography mode on the platform.

Syntax

```
[no] fips mode enable
```

To disable the FIPS cryptography mode, use the `no fips mode enable` command.

Default

Disabled

Command Modes

CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell (conf)#fips mode enable
WARNING: Enabling FIPS mode will close all SSH/Telnet
connection, restart those servers, and destroy all configured
host keys.
proceed (y/n) ? y
Dell (conf)#
```

Related Commands

ssh — opens an SSH connection specifying the hostname, username, port number, and version of the SSH client.

show fips status

Displays the status of the FIPS mode.

Syntax

```
show fips status
```

Defaults

None

Command Modes

EXEC

Command History	Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show fips status
FIPS Mode: Enabled
Dell#
```

show ip ssh

Display information about established SSH sessions

Syntax `show ip ssh`

Defaults none

Command Modes

EXEC

EXEC Privilege

Command History	Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show ip ssh
SSH server                             : enabled.
SSH server version               : v1 and v2.
Password Authentication      : enabled.
Hostbased Authentication   : disabled.
RSA Authentication               : disabled.
 Vty        Encryption    HMAC         Remote IP
 1            3des-cbc        hmac-md5 10.1.20.48
 2            3des-cbc        hmac-md5 10.1.20.48
```

With FIPS Mode enabled:

```
Dell#show ip ssh
SSH server                             : enabled.
SSH server version               : v2.
Password Authentication      : enabled.
Hostbased Authentication   : disabled.
RSA Authentication               : disabled.
 Vty     Encryption    HMAC           Remote IP
 0         aes128-cbc    hmac-sha1  10.11.8.13
 1         aes128-cbc    hmac-sha1  10.1.20.48
```

ssh

Open an SSH connection specifying the hostname, username, port number, and version of the SSH client.

Syntax

```
ssh {hostname | ipv4 address | ipv6 address} [-c encryption
cipher | -l username | -m HMAC alogorithm | -p port-number | -v
{1|2}]
```

Parameters

hostname	(OPTIONAL) Enter the IP address or the hostname of the remote device.
ipv4 address	(OPTIONAL) Enter the IP address in dotted decimal format A.B.C.D.
ipv6 address prefix-length	(OPTIONAL) Enter the IPv6 address in the x:x:x:x::x format then the prefix length in the /x format. The range is from /0 to /128 **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
-c encryption cipher	Enter the following encryption cipher to use. (For v2 clients only.) Without the FIPS mode enabled: • `3des-cbc`: Force ssh to use 3des-cbc encryption cipher. With the FIPS mode enabled: • `aes128-cbc`: Force ssh to use the aes128–cbc encryption cipher. • `aes256-cbc`: Force ssh to use the aes256–cbc encryption cipher.
-l username	(OPTIONAL) Enter the keyword `–l` then the user name used in this SSH session. The default is the user name of the user associated with the terminal.
-m HMAC algorithm	Enter one of the following HMAC algorithms to use. (For v2 clients only.): Without the FIPS mode enabled: • `hmac-sha1`: Force ssh to use the hmac-sha1 HMAC algorithm. • `hmac-sha1-96`: Force ssh to use the hmac-sha1–96 HMAC algorithm. • `hmac-md5`: Force ssh to use the hmac-md5 HMAC algorithm. • `hmac-md5-96`: Force ssh to use the hmac-md5–96 HMAC algorithm. With the FIPS mode enabled: • `hmac-sha1`: Force ssh to use the hmac-sha1 HMAC algorithm.

- `hmac-sha1-96`: Force ssh to use the hmac-sha1–96 HMAC algorithm.

-p port-number	(OPTIONAL) Enter the keyword `–p` then the port number. The range is 1 to 65536 The default is 22
-v {1|2}	(OPTIONAL) Enter the keyword `–v` then the SSH version 1 or 2. The default: The version from the protocol negotiation. NOTE: If the FIPS mode is enabled, this option does not display in the output.

Defaults
As indicated above.

Command Modes
EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Example

If FIPS mode is not enabled:

```
Dell#ssh 10.11.8.12 ?
-c        Encryption cipher to use (for v2 client
-l     User name option
-m     HMAC algorithm to use (for v2 clients only)
-p     SSH server port option (default 22)
-v     SSH protocol version
<cr>
Dell#ssh 10.11.8.12 -c ?
3des-cbc     Force ssh to use 3des-cbc encryption cipher
Dell#ssh 10.11.8.12 -m ?
hmac-sha1     Force ssh to use hmac-sha1 HMAC algorithm
hmac-sha1-96     Force ssh to use hmac-sha1-96 HMAC algorithm
hmac-md5     Force ssh to use hmac-md5 HMAC algorithm
hmac-md5-96     Force ssh to use hmac-md5-96 HMAC algorithm
```

With FIPS mode enabled:

```
Dell#ssh 10.11.8.12 ?
-c        Encryption cipher to use (for v2 client
-l     User name option
-m     HMAC algorithm to use (for v2 clients only)
-p     SSH server port option (default 22)
<cr>
Dell#ssh 10.11.8.12 -c ?
aes128-cbc     Force ssh to use aes128-cbc encryption cipher
aes256-cbc     Force ssh to use aes256-cbc encryption cipher
Dell#ssh 10.11.8.12 -m ?
hmac-sha1     Force ssh to use hmac-sha1 HMAC algorithm
hmac-sha1-96     Force ssh to use hmac-sha1-96 HMAC algorithm
```

17

FIP Snooping

In a converged Ethernet network, an MXL Switch can operate as an intermediate Ethernet bridge to snoop on Fibre Channel over Ethernet initialization protocol (FIP) packets during the login process on Fibre Channel over Ethernet (FCoE) forwarders (FCFs).

Acting as a transit FIP snooping bridge, the switch uses dynamically-created ACLs to permit only authorized FCoE traffic to be transmitted between an FCoE end-device and an FCF. The following Dell Networking Operating System (OS) commands are used to configure and verify the FIP snooping feature.

clear fip-snooping database interface vlan

Clear FIP snooping information on a VLAN for a specified FCoE MAC address, ENode MAC address, or FCF MAC address, and remove the corresponding ACLs FIP snooping generates.

Syntax

```
clear fip-snooping database interface vlan vlan-id {fcoe-mac-address | enode-mac-address | fcf-mac-address}
```

Parameters

fcoe-mac-address	Enter the FCoE MAC address to be cleared of FIP snooping information.
enode-mac-address	Enter the ENode MAC address to be cleared of FIP snooping information.
fcf-mac-address	Enter the FCF MAC address to be cleared of FIP snooping information.

Command Modes: EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

clear fip-snooping statistics

Clears the statistics on the FIP packets snooped on all VLANs, a specified VLAN, or a specified port interface.

Syntax

```
clear fip-snooping statistics [interface vlan vlan-id |
interface port-type port/slot | interface port-channel port-
channel-number]
```

Parameters

vlan-id	Enter the VLAN ID of the FIP packet statistics to be cleared.
port-type port/slot	Enter the port-type and slot number of the FIP packet statistics to be cleared.
port-channel-number	Enter the port channel number of the FIP packet statistics to be cleared.

Command Modes

EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

clear fip-snooping statistics

Clears the statistics on the FIP packets snooped on all VLANs, a specified VLAN, or a specified port interface.

Syntax

```
clear fip-snooping statistics [interface vlan vlan-id |
interface port-type port/slot | interface port-channel port-
channel-number]
```

Parameters

vlan-id	Enter the VLAN ID of the FIP packet statistics to be cleared.
port-type port/slot	Enter the port-type and slot number of the FIP packet statistics to be cleared.
port-channel-number	Enter the port channel number of the FIP packet statistics to be cleared.

Command Modes

EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

feature fip-snooping

Enable FCoE transit and FIP snooping on a switch.

Syntax	`feature fip-snooping` To disable the FCoE transit feature, use the `no feature fip-snooping` command.
Defaults	Disabled
Command Modes	CONFIGURATION
Command History	**Version 9.2(0.0)**: Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only. **Version 8.3.16.1**: Introduced on the MXL 10/40GbE Switch IO Module.

fip-snooping enable

Enable FIP snooping on all VLANs or on a specified VLAN.

Syntax	`fip-snooping enable` To disable the FIP snooping feature on all or a specified VLAN, use the `no fip-snooping enable` command.
Defaults	FIP snooping is disabled on all VLANs.
Command Modes	• CONFIGURATION • VLAN INTERFACE
Command History	**Version 9.2(0.0)**: Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only. **Version 8.3.16.1**: Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	The maximum number of FCFs supported per FIP snooping-enabled VLAN is four. The maximum number of FIP snooping sessions supported per ENode server is 16.

fip-snooping fc-map

Configure the FC-MAP value FIP snooping uses on all VLANs.

Syntax	`fip-snooping fc-map fc-map-value` To return the configured FM-MAP value to the default value, use the `no fip-snooping fc-map` command.
Parameters	*fc-map-value* — Enter the FC-MAP value FIP snooping uses. The range is from 0EFC00 to 0EFCFF.
Defaults	**0x0EFC00**
Command Modes	CONFIGURATION VLAN INTERFACE
Command History	Version 9.2(0.0) — Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only. Version 8.3.16.1 — Introduced on the MXL 10/40GbE Switch IO Module.

fip-snooping port-mode fcf

Configure the port for bridge-to-FCF links.

Syntax	`fip-snooping port-mode fcf` To disable the bridge-to-FCF link on a port, use the `no fip-snooping port-mode fcf` command.
Command Modes	INTERFACE
Command History	Version 9.2(0.0) — Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only. Version 8.3.16.1 — Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	The maximum number of FCFs supported per FIP snooping-enabled VLAN is four.

show fip-snooping config

Display the FIP snooping status and configured FC-MAP values.

Syntax `show fip-snooping config`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell# show fip-snooping config
FIP Snooping Feature enabled Status: Enabled
FIP Snooping Global enabled Status: Enabled
Global FC-MAP Value: 0X0EFC00

FIP Snooping enabled VLANs
VLAN   Enabled   FC-MAP
----   -------   --------
100    TRUE      0X0EFC00
```

show fip-snooping enode

Display information on the ENodes in FIP-snooped sessions, including the ENode interface and MAC address, FCF MAC address, VLAN ID and FC-ID.

Syntax `show fip-snooping enode [enode-mac-address]`

Parameters

enode-mac-address	Enter the MAC address of the ENodes to display.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on MXL 10/40GbE Switch IO Module

Usage Information

The following describes the `show fip-snooping enode` command shown in the following example.

Field	Description
ENode MAC	MAC address of the ENode.
ENode Interface	Slot/ port number of the interface connected to the ENode.
FCF MAC	MAC address of the FCF.
VLAN	VLAN ID number the session uses.

Field	Description
FC-ID	Fibre Channel session ID the FCF assigns.

Example

```
Dell# show fip-snooping enode
Enode MAC         Enode Interface FCF MAC           VLAN FC-ID
---------         --------------- -------            ---- -----
d4:ae:52:1b:e3:cd Te 0/11         54:7f:ee:37:34:40 100
62:00:11
```

show fip-snooping fcf

Display information on the FCFs in FIP-snooped sessions, including the FCF interface and MAC address, FCF interface, VLAN ID, FC-MAP value, FKA advertisement period, and number of ENodes connected.

Syntax

`show fip-snooping fcf [`*`fcf-mac-address`*`]`

Parameters

fcf-mac-address	Enter the MAC address of the FCF to display.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show fip-snooping fcf` command shown in the following example.

Field	Description
FCF MAC	MAC address of the FCF.
FCF Interface	Slot/port number of the interface to which the FCF is connected.
VLAN	VLAN ID number the session uses.
FC-MAP	FC-Map value the FCF advertises.
ENode Interface	Slot/ number of the interface connected to the ENode.
FKA_ADV_PERIOD	Time (in milliseconds) during which FIP keep-alive advertisements transmit.
No of ENodes	Number of ENodes connected to the FCF.
FC-ID	Fibre Channel session ID the FCF assigns.

Example

```
Dell# show fip-snooping fcf
FCF MAC           FCF Interface VLAN  FC-MAP   FKA_ADV_PERIOD
No. of Enodes
-------           ------------- ---- ------    --------------
```

```
-------------
54:7f:ee:37:34:40 Po 22         100  0e:fc:00 4000           2
```

show fip-snooping sessions

Display information on FIP-snooped sessions on all VLANs or a specified VLAN, including the ENode interface and MAC address, the FCF interface and MAC address, VLAN ID, FCoE MAC address and FCoE session ID number (FC-ID), worldwide node name (WWNN) and the worldwide port name (WWPN).

Syntax `show fip-snooping sessions [interface vlan vlan-id]`

Parameters

vlan-id	Enter the vlan-id of the specified VLAN to display.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show fip-snooping sessions` command shown in the following example.

Field	Description
ENode MAC	MAC address of the ENode.
ENode Interface	Slot/ port number of the interface connected to the ENode.
FCF MAC	MAC address of the FCF.
FCF Interface	Slot/ port number of the interface to which the FCF is connected.
VLAN	VLAN ID number the session uses.
FCoE MAC	MAC address of the FCoE session the FCF assigns.
FC-ID	Fibre Channel ID the FCF assigns.
Port WWPN	Worldwide port name of the CNA port.
Port WWNN	Worldwide node name of the CNA port.

Example

```
Dell#show fip-snooping sessions
Enode MAC          Enode Intf  FCF MAC           FCF Intf VLAN
aa:bb:cc:00:00:00  Te 0/42    aa:bb:cd:00:00:00 Te 0/43  100
aa:bb:cc:00:00:00  Te 0/42    aa:bb:cd:00:00:00 Te 0/43  100
aa:bb:cc:00:00:00  Te 0/42    aa:bb:cd:00:00:00 Te 0/43  100
aa:bb:cc:00:00:00  Te 0/42    aa:bb:cd:00:00:00 Te 0/43  100
aa:bb:cc:00:00:00  Te 0/42    aa:bb:cd:00:00:00 Te 0/43  100

FCoE MAC           FC-ID      Port WWPN                  Port
WWNN
0e:fc:00:01:00:01  01:00:01 31:00:0e:fc:00:00:00:00
```

```
21:00:0e:fc:00:00:00:00
0e:fc:00:01:00:02  01:00:02 41:00:0e:fc:00:00:00:00
21:00:0e:fc:00:00:00:00
0e:fc:00:01:00:03  01:00:03 41:00:0e:fc:00:00:00:01
21:00:0e:fc:00:00:00:00
0e:fc:00:01:00:04  01:00:04 41:00:0e:fc:00:00:00:02
21:00:0e:fc:00:00:00:00
0e:fc:00:01:00:05  01:00:05 41:00:0e:fc:00:00:00:03
21:00:0e:fc:00:00:00:00
```

show fip-snooping statistics

Display statistics on the FIP packets snooped on all interfaces, including VLANs, physical ports, and port channels.

Syntax

```
show fip-snooping statistics [interface vlan vlan-id |
interface port-type port/slot | interface port-channel port-
channel-number]
```

Parameters

vlan-id	Enter the VLAN ID of the FIP packet statistics displays.
port-type port/slot	Enter the port-type and slot number of the FIP packet statistics displays.
port-channel-number	Enter the port channel number of the FIP packet statistics displays.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show fip-snooping statistics` command shown in the following example.

Field	Description
Number of VLAN Requests	Number of FIP-snoop VLAN request frames received on the interface.
Number of VLAN Notifications	Number of FIP-snoop VLAN notification frames received on the interface.
Number of Multicast Discovery Solicits	Number of FIP-snoop multicast discovery solicit frames received on the interface.
Number of Unicast Discovery Solicits	Number of FIP-snoop unicast discovery solicit frames received on the interface.

Field	Description
Number of FLOGI	Number of FIP-snoop FLOGI request frames received on the interface.
Number of FDISC	Number of FIP-snoop FDISC request frames received on the interface.
Number of FLOGO	Number of FIP-snoop FLOGO frames received on the interface
Number of ENode Keep Alives	Number of FIP-snoop ENode keep-alive frames received on the interface.
Number of VN Port Keep Alives	Number of FIP-snoop VN port (Virtual N-port) keep-alive frames received on the interface
Number of Multicast Discovery Advertisements	Number of FIP-snoop multicast discovery advertisements received on the interface.
Number of Unicast Discovery Advertisements	Number of FIP-snoop unicast discovery advertisements received on the interface.
Number of FLOGI Accepts	Number of FIP FLOGI accept frames received on the interface.
Number of FLOGI Rejects	Number of FIP FLOGI reject frames received on the interface.
Number of FDISC Accepts	Number of FIP FDISC accept frames received on the interface.
Number of FDISC Rejects	Number of FIP FDISC reject frames received on the interface.
Number of FLOGO Accepts	Number of FIP FLOGO accept frames received on the interface.
Number of FLOGO Rejects	Number of FIP FLOGO reject frames received on the interface.
Number of CVLs	Number of FIP clear virtual link frames received on the interface.
Number of FCF Discovery Timeouts	Number of FCF discovery timeouts that occurred on the interface.
Number of VN Port Session Timeouts	Number of VN port session timeouts that occurred on the interface.
Number of Session failures	Number of session failures due to hardware configuration that occurred on the interface.

Field	Description
due to Hardware Config	

Example

```
Dell# show fip-snooping statistics interface vlan 100
Number of Vlan Requests                        :0
Number of Vlan Notifications                   :0
Number of Multicast Discovery Solicits         :2
Number of Unicast Discovery Solicits           :0
Number of FLOGI                                :2
Number of FDISC                                :16
Number of FLOGO                                :0
Number of Enode Keep Alive                     :9021
Number of VN Port Keep Alive                   :3349
Number of Multicast Discovery Advertisement :4437
Number of Unicast Discovery Advertisement   :2
Number of FLOGI Accepts                        :2
Number of FLOGI Rejects                        :0
Number of FDISC Accepts                        :16
Number of FDISC Rejects                        :0
Number of FLOGO Accepts                        :0
Number of FLOGO Rejects                        :0
Number of CVL                                  :0
Number of FCF Discovery Timeouts               :0
Number of VN Port Session Timeouts             :0
Number of Session failures due to Hardware Config :0
Dell(conf)#

Dell# show fip-snooping statistics int tengigabitethernet 0/11
Number of Vlan Requests                        :1
Number of Vlan Notifications                   :0
Number of Multicast Discovery Solicits         :1
Number of Unicast Discovery Solicits           :0
Number of FLOGI                                :1
Number of FDISC                                :16
Number of FLOGO                                :0
Number of Enode Keep Alive                     :4416
Number of VN Port Keep Alive                   :3136
Number of Multicast Discovery Advertisement :0
Number of Unicast Discovery Advertisement   :0
Number of FLOGI Accepts                        :0
Number of FLOGI Rejects                        :0
Number of FDISC Accepts                        :0
Number of FDISC Rejects                        :0
Number of FLOGO Accepts                        :0
Number of FLOGO Rejects                        :0
Number of CVL                                  :0
Number of FCF Discovery Timeouts               :0
Number of VN Port Session Timeouts             :0
Number of Session failures due to Hardware Config :0
```

Example (Port Channel)

```
Dell# show fip-snooping statistics interface port-channel 22
Number of Vlan Requests                        :0
Number of Vlan Notifications                   :2
Number of Multicast Discovery Solicits         :0
Number of Unicast Discovery Solicits           :0
Number of FLOGI                                :0
Number of FDISC                                :0
Number of FLOGO                                :0
Number of Enode Keep Alive                     :0
Number of VN Port Keep Alive                   :0
Number of Multicast Discovery Advertisement :4451
Number of Unicast Discovery Advertisement   :2
Number of FLOGI Accepts                     :2
Number of FLOGI Rejects                     :0
Number of FDISC Accepts                     :16
Number of FDISC Rejects                     :0
Number of FLOGO Accepts                     :0
Number of FLOGO Rejects                     :0
Number of CVL                               :0
Number of FCF Discovery Timeouts            :0
Number of VN Port Session Timeouts          :0
Number of Session failures due to Hardware Config :0
```

show fip-snooping system

Display information on the status of FIP snooping on the switch (enabled or disabled), including the number of FCoE VLANs, FCFs, ENodes, and currently active sessions.

Syntax `show fip-snooping system`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell# show fip-snooping system
Global Mode : Enabled
FCOE VLAN List (Operational) : 1, 100
FCFs                         : 1
Enodes                       : 2
Sessions                     : 17
```

show fip-snooping vlan

Display information on the FCoE VLANs on which FIP snooping is enabled.

Syntax `show fip-snooping vlan`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell# show fip-snooping vlan
* = Default VLAN
VLAN FC-MAP    FCFs Enodes Sessions
---- ------ ---- ------ --------
```

```
*1    -         -    -      -
100   0X0EFC00 1    2      17
```

18

Force10 Resilient Ring Protocol (FRRP)

Force10 resilient ring protocol (FRRP) is supported on Dell Networking MXL 10/40GbE Switch IO Module.

FRRP is a proprietary protocol for that offers fast convergence in a Layer 2 network without having to run the spanning tree protocol (STP). The resilient ring protocol is an efficient protocol that transmits a high-speed token across a ring to verify the link status. All the intelligence is contained in the master node with practically no intelligence required of the transit mode.

Important Points to Remember

- FRRP is media- and speed-independent.
- FRRP is a Dell Networking proprietary protocol that does not interoperate with any other vendor.
- Spanning Tree must be disabled on both primary and secondary interfaces before Resilient Ring protocol is enabled.
- A virtual local area network (VLAN) configured as the control VLAN for a ring cannot be configured as a control or member VLAN for any other ring.
- Member VLANs across multiple rings are not supported in Master nodes.
- If multiple rings share one or more member VLANs, they cannot share any links between them.
- Each ring can have only one Master node; all others are Transit nodes.

clear frrp

Clear the FRRP statistics counters.

Syntax `clear frrp [ring-id]`

Parameters

ring-id	(Optional) Enter the ring identification number. The range is from 1 to 255.

Defaults none

Command Modes EXEC

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information Executing this command without the optional `ring-id` command clears the statistics counters on all the available rings. The system requires a command line confirmation before the command executes. This command clears the following counters:

- hello Rx and Tx counters
- Topology change Rx and Tx counters
- The number of state change counters

Example

```
Dell#clear frrp

Clear frrp statistics counter on all ring [confirm] yes

Dell#clear frrp 4

Clear frrp statistics counter for ring 4 [confirm] yes

Dell#
```

Related Commands

show frrp — displays the resilient ring protocol configuration.

debug frrp

Clear the FRRP statistics counters.

Syntax

`debug frrp {event | packet | detail} [ring-id] [count number]`

To disable debugging, use the `no debug frrp {event | packet | detail} {ring-id} [countnumber]` command.

Parameters

event	Enter the keyword `event` to display debug information related to ring protocol transitions.
packet	Enter the keyword `packet` to display brief debug information related to control packets.
detail	Enter the keyword `detail` to display detailed debug information related to the entire ring protocol packets.
ring-id	(Optional) Enter the ring identification number. The range is from 1 to 255.
count *number*	Enter the keyword `count` then the number of debug outputs. The range is from 1 to 65534.

Defaults

Disabled.

Command Modes

CONFIGURATION (conf-frrp)

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Because the resilient ring protocol can potentially transmit 20 packets per interface, restrict debug information.

description

Enter an identifying description of the ring.

Syntax

`description Word`

To remove the ring description, use the `no description [Word]` command.

Parameters

Word	Enter a description of the ring. Maximum: 255 characters.

Defaults none

Command Modes CONFIGURATION (conf-frrp)

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

disable

Disable the resilient ring protocol.

Syntax

`disable`

To enable the Resilient Ring Protocol, use the `no disable` command.

Defaults **Disabled**

Command Modes CONFIGURATION (conf-frrp)

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

interface

Configure the primary, secondary, and control-vlan interfaces.

Syntax

`interface {primary interface secondary interface control-vlan vlan-id}`

To return to the default, use the `no interface {primary interface secondary interface control-vlan vlan-id}` command.

Parameters

primary *interface*	Enter the keyword `primary` to configure the primary interface then one of the following interfaces and slot/port information:

- `Fast Ethernet interface`: enter the keyword `FastEthernet` then the slot/port information.
- `Port Channel interface`: enter the keyword `port-channel` then a number. The range is from 1 to 128.
- `10-Gigabit Ethernet interface`: enter the keyword `TenGigabitEthernet` then the slot/port information
- `40-Gigabit Ethernet interface`: enter the keyword `fortyGigE` then the slot/port information

secondary *interface*

Enter the keyword `secondary` to configure the secondary interface then one of the following interfaces and slot/port information:

- `Fast Ethernet interface`: enter the keyword `FastEthernet` then the slot/port information.
- `Port Channel interface`: enter the keyword `port-channel` then a number. The range is from 1 to 128.
- `10-Gigabit Ethernet interface`: enter the keyword `TenGigabitEthernet` then the slot/port information
- `40-Gigabit Ethernet interface`: enter the keyword `fortyGigE` then the slot/port information

control-vlan *vlan-id*

Enter the keyword `control-vlan` then the VLAN ID. The range is from 1 to 4094.

Defaults

none

Command Modes

CONFIGURATION (conf-frrp)

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

This command causes the Ring Manager to take ownership of the two ports after IFM validates the configuration. Ownership is relinquished for a port only when the interface does not play a part in any control VLAN, that is, the interface does not belong to any ring.

Related Commands

show frrp — displays the resilient ring protocol configuration information.

member-vlan

Specify the member VLAN identification numbers.

Syntax

`member-vlan {vlan-range}`

To return to the default, use the `no member-vlan [vlan-range]` command.

Parameters

vlan-range	Enter the member VLANs using VLAN IDs (separated by commas), a range of VLAN IDs (separated by a hyphen), a single VLAN ID, or a combination. For example: VLAN IDs (comma-separated): 3, 4, 6. Range (hyphen-separated): 5-10. Combination: 3, 4, 5-10, 8.

Defaults none

Command Modes CONFIGURATION (conf-frrp)

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

mode

Set the Master or Transit mode of the ring.

Syntax `mode {master | transit}`

To reset the mode, use the `no mode {master | transit}` command.

Parameters

master	Enter the keyword `master` to set the Ring node to Master mode.
transit	Enter the keyword`transit` to set the Ring node to Transit mode.

Defaults Mode None

Command Modes CONFIGURATION (conf-frrp)

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

protocol frrp

Enter the Resilient Ring Protocol and designate a ring identification.

Syntax `protocol frrp {ring-id}`

To exit the ring protocol, use the `no protocol frrp {ring-id}` command.

Parameters

ring-id	Enter the ring identification number. The range is from 1 to 255.

Defaults	none
Command Modes	CONFIGURATION
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	This command places you into the resilient ring protocol. After executing this command, the command line prompt changes to `conf-frrp`.

show frrp

Display the resilient ring protocol configuration.

Syntax `show frrp [ring-id [summary]] | [summary]`

Parameters

ring-id	Enter the ring identification number. The range is from 1 to 255
summary	(OPTIONAL) Enter the keyword `summary` to view just a summarized version of the Ring configuration.

Defaults	none
Command Modes	EXEC
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Executing this command without the optional `ring-id` command clears the statistics counters on all the available rings. The system requires a command line confirmation before the command executes. This command clears the following counters:

- hello Rx and Tx counters
- Topology change Rx and Tx counters
- The number of state change counters

Example (Summary)

```
Dell#show frrp summary
Ring-ID State Mode  Ctrl_Vlan Member_Vlans
---------------------------------------------
2       UP   Master   2        11-20, 25,27-30
31      UP   Transit  31       40-41
50      Down Transit  50       32
Dell#
```

Example (1)

```
Dell#show frrp 1
Ring protocol 1 is in Master mode
Ring Protocol Interface:
Primary : GigabitEthernet 0/16 State: Forwarding
```

```
Secondary: Port-channel 100 State: Blocking
Control Vlan: 1
Ring protocol Timers: Hello-Interval 50 msec Dead-Interval 150
msec
Ring Master's MAC Address is 00:01:e8:13:a3:19
Topology Change Statistics: Tx:110 Rx:45
Hello Statistics: Tx:13028 Rx:12348
Number of state Changes: 34
Member Vlans: 1000-1009
Dell#
```

Example (2 Summary)

```
Dell#show frrp 2 summary
```

```
Dell#show frrp 2 summary
Ring-ID State Mode  Ctrl_Vlan Member_Vlans
----------------------------------------------
2       Up    Master 2        11-20, 25, 27-30
Dell#
```

Related Commands

protocol frrp — enters the resilient ring protocol and designate a ring identification.

timer

Set the hello interval or dead interval for the Ring control packets.

Syntax

`timer {hello-interval` *`milliseconds`*`}| {dead-interval` *`milliseconds`*`}`

To remove the timer, use the `no timer {hello-interval [`*`milliseconds`*`]}| {dead-interval` *`milliseconds`*`}` command.

Parameters

hello-interval *milliseconds*	Enter the keyword `hello-interval` then the time, in milliseconds, to set the hello interval of the control packets. The milliseconds must be entered in increments of 50 millisecond; for example, 50, 100, 150, and so on. If an invalid value is entered, an error message is generated. The range is from 50 to 2000 ms. Default: **500 ms**.
dead-interval *milliseconds*	Enter the keyword `dead-interval` then the time, in milliseconds, to set the dead interval of the control packets. The range is from 50 to 6000 ms. Default: **1500 ms**. NOTE: The configured dead interval must be at least three times the hello interval.

Defaults

- **500 ms** for `hello-interval` *`milliseconds`*
- **1500 ms** for `dead-interval`*`milliseconds`*

Command Modes

CONFIGURATION (conf-frrp)

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The `hello interval` command is the interval at which ring frames are generated from the primary interface of the master node. The `dead interval` command is the time that elapses before a time-out occurs.

19

GARP VLAN Registration (GVRP)

The Dell Networking Operating System (OS) supports the basic GVRP commands.

The generic attribute registration protocol (GARP) mechanism allows the configuration of a GARP participant to propagate through a network quickly. A GARP participant registers or de-registers its attributes with other participants by making or withdrawing declarations of attributes. At the same time, based on received declarations or withdrawals, GARP handles attributes of other participants.

GVRP enables a device to propagate local virtual local area network (VLAN) registration information to other participant devices and dynamically update the VLAN registration information from other devices. The registration information updates local databases regarding active VLAN members and through which port the VLANs can be reached.

GVRP ensures that all participants on a bridged LAN maintain the same VLAN registration information. The VLAN registration information propagated by GVRP includes both manually configured local static entries and dynamic entries from other devices.

GVRP participants have the following components:

- The GVRP application
- GARP information propagation (GIP)
- GARP information declaration (GID)

Important Points to Remember

- GVRP is supported on Layer 2 ports only.
- All VLAN ports added by GVRP are tagged.
- GVRP is supported on untagged ports belonging to a default VLAN and tagged ports.
- GVRP cannot be enabled on untagged ports belonging to a non-default VLAN *unless* native VLAN is turned on.
- GVRP requires end stations with dynamic access network interface controller (NICs).
- Based on updates from GVRP-enabled devices, GVRP allows the system to dynamically create a port-based VLAN (unspecified) with a specific VLAN ID and a specific port.
- On a port-by-port basis, GVRP allows the system to learn about GVRP updates to an existing port-based VLAN with that VLAN ID and IEEE 802.1Q tagging.
- GVRP allows the system to send dynamic GVRP updates about your existing port-based VLAN.
- GVRP updates are not sent to any blocked spanning tree protocol (STP) ports. GVRP operates only on ports that are in the forwarding state.
- GVRP operates only on ports that are in the STP forwarding state. If you enable GVRP, a port that changes to the STP Forwarding state automatically begin to participate in GVRP. A port that changes to an STP state other than forwarding no longer participates in GVRP.

- VLANs created dynamically with GVRP exist only as long as a GVRP-enabled device is sending updates. If the devices no longer send updates, or GVRP is disabled, or the system is rebooted, all dynamic VLANs are removed.
- GVRP manages the active topology, not non-topological data such as VLAN protocols. If a local bridge must classify and analyze packets by VLAN protocols, manually configure protocol-based VLANs, and simply rely on GVRP for VLAN updates. But if the local bridge must know only how to reach a given VLAN, then GVRP provides all necessary information.
- The VLAN topologies that GVRP learns are treated differently from VLANs that are statically configured. The GVRP dynamic updates are not saved in NVRAM, while static updates are saved in NVRAM. When GVRP is disabled, the system deletes all VLAN interfaces that were learned through GVRP and leaves unchanged all VLANs that were manually configured.

clear gvrp statistics

Clear GVRP statistics on an interface.

Syntax

```
clear gvrp statistics interface interface
```

Parameters

interface *interface*	Enter the following keywords and slot/port or number information: • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

Defaults

none

Command Modes

EXEC

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

show gvrp statistics — displays the GVRP statistics.

debug gvrp

Enable debugging on GVRP.

Syntax

```
debug gvrp {config | events | pdu}
```

To disable debugging, use the `no debug gvrp {config | events | pdu}` command.

Parameters	config	Enter the keyword `config` to enable debugging on the GVRP configuration.
	event	Enter the keyword `event` to enable debugging on the JOIN/LEAVE events.
	pdu	Enter the keyword `pdu` then one of the following Interface keywords and slot/port or number information: • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

Defaults Disabled.

Command Modes EXEC

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

disable

Globally disable GVRP.

Syntax `disable`

To re-enable GVRP, use the `no disable` command.

Defaults Enabled.

Command Modes CONFIGURATION-GVRP

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

gvrp enable — enables GVRP on physical interfaces and LAGs.

protocol gvrp — access GVRP protocol.

garp timers

Set the intervals (in milliseconds) for sending GARP messages.

Syntax

`garp timers {join | leave | leave-all}`

To return to the previous setting, use the `no garp timers {join | leave | leave-all}` command.

Parameters

join	Enter the keyword `join` then the number of milliseconds to configure the join time. The range is from 100 to 147483647 milliseconds. The default is **200 milliseconds**. ✎ NOTE: Designate the milliseconds in multiples of 100.
leave	Enter the keyword `leave` then the number of milliseconds to configure the leave time. The range is from 100 to 2147483647 milliseconds. The default is **600 milliseconds**. ✎ NOTE: Designate the milliseconds in multiples of 100.
leave-all	Enter the keywords `leave-all` then the number of milliseconds to configure the leave-all time. The range is from 100 to 2147483647 milliseconds. The default is 1000 milliseconds. ✎ NOTE: Designate the milliseconds in multiples of 100.

Defaults

As above.

Command Modes

CONFIGURATION-GVRP

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

- **Join Timer** — `Join` messages announce the willingness to register some attributes with other participants. For reliability, each GARP application entity sends a `Join` message twice and uses a join timer to set the sending interval.
- **Leave Timer** — `Leave` announces the willingness to de-register with other participants. Together with `Join`, `Leave` messages help GARP participants complete attribute reregistration and de-registration. The leave timer starts after receipt of a leave message sent for de-registering some attribute information. If a `Join` message is *not* received before the `Leave` time expires, the GARP application entity removes the attribute information as requested.
- **Leave All Timer** — The `Leave All` timer starts when a GARP application entity starts. When this timer expires, the entity sends a `Leave-all` message so that other entities can reregister their attribute information. Then the `Leave-all` time begins again.

Related Commands

show garp timers — displays the current GARP times.

gvrp enable

Enable GVRP on physical interfaces and LAGs.

Syntax	`gvrp enable` To disable GVRP on the interface, use the `no gvrp enable` command.
Defaults	Disabled.
Command Modes	CONFIGURATION-INTERFACE
Command History	Version 8.3.16.1 — Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	disable — globally disables GVRP.

gvrp registration

Configure the GVRP register type.

Syntax	`gvrp registration {fixed | normal | forbidden}` To return to the default, use the `gvrp register normal` command.

Parameters

fixed	Enter the keyword `fixed` then the VLAN range in a comma-separated VLAN ID set.
normal	Enter the keyword `normal` then the VLAN range in a comma-separated VLAN ID set. This setting is the default.
forbidden	Enter the keyword `forbidden` then the VLAN range in a comma-separated VLAN ID set.

Defaults	**normal**
Command Modes	CONFIGURATION-INTERFACE
Command History	Version 8.3.16.1 — Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

`Fixed` registration prevents an interface, configured using the command line, to belong to a VLAN (static configuration) from being unconfigured when it receives a `Leave` message. Therefore, Registration mode on that interface is fixed.

`Normal` registration is the default registration. The port's membership in the VLAN depends on GVRP. The interface becomes a member of a VLAN after learning about the VLAN through GVRP. If the VLAN is removed from the port that sends GVRP advertisements to this device, the port stops being a member of the VLAN.

To advertise or learn about VLANs through GVRP, use the `forbidden` command when you do not want the interface.

Related Commands	show gvrp — displays the GVRP configuration including the registration.

protocol gvrp

Access GVRP protocol — (config-gvrp)#.

Syntax	`protocol gvrp`
Defaults	Disabled.
Command Modes	CONFIGURATION
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	disable — globally disables GVRP.

show config

Display the global GVRP configuration.

Syntax	`show config`
Command Modes	CONFIGURATION-GVRP
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	gvrp enable — enables GVRP on physical interfaces and LAGs. protocol gvrp — accesses the GVRP protocol.

show garp timers

Display the GARP timer settings for sending GARP messages.

Syntax	`show garp timers`

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show garp timers
GARP Timers      Value (milliseconds)
----------------------------------------
Join Timer         200
Leave Timer        600
LeaveAll Timer     10000
Dell#
```

Related Commands

garp timers — sets the intervals (in milliseconds) for sending GARP messages.

show gvrp

Display the GVRP configuration.

Syntax `show gvrp [brief | interface]`

Parameters

brief	(OPTIONAL) Enter the keyword `brief` to display a brief summary of the GVRP configuration.
interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

If no ports are GVRP participants, the message output changes from `GVRP Participants running on <port_list>` to `GVRP Participants running on no ports.`

Example

```
R3#show gvrp brief
GVRP Feature is currently enabled.
Port                GVRP Status      Edge-Port
---------------------------------------------
Gi 3/0              Disabled          No
Gi 3/1              Disabled          No
Gi 3/2              Enabled           No
Gi 3/3              Disabled          No
Gi 3/4              Disabled          No
Gi 3/5              Disabled          No
Gi 3/6              Disabled          No
Gi 3/7              Disabled          No
Gi 3/8              Disabled          No
R3#show gvrp brief
```

Related Commands

show gvrp statistics — displays the GVRP statistics.

clear gvrp statistics

Clear GVRP statistics on an interface.

Syntax

```
clear gvrp statistics {interface interface | summary}
```

Parameters

interface *interface*	Enter the following keywords and slot/port or number information: • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
summary	Enter the keyword `summary` to display just a summary of the GVRP statistics.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Invalid messages/attributes skipped can occur in the following cases:

- The incoming GVRP PDU has an incorrect length.
- “End of PDU” was reached before the complete attribute could be parsed.
- The Attribute Type of the attribute that was being parsed was not the GVRP VID Attribute Type (0x01).

- The attribute that was being parsed had an invalid attribute length.
- The attribute that was being parsed had an invalid GARP event.
- The attribute that was being parsed had an invalid VLAN ID. The valid range is 1 - 4095.

A failed registration can occur for the following reasons:

- Join requests were received on a port that was blocked from learning dynamic VLANs (GVRP Blocking state).
- An entry for a new GVRP VLAN could not be created in the GVRP database.

Example

```
Dell#show gvrp statistics int tengig 1/0

Join Empty Received: 0
Join In Received: 0
Empty Received: 0
LeaveIn Received: 0
Leave Empty Received: 0
Leave All Received: 40
Join Empty Transmitted: 156
Join In Transmitted: 0
Empty Transmitted: 0
Leave In Transmitted: 0
Leave Empty Transmitted: 0
Leave All Transmitted: 41
Invalid Messages/Attributes skipped: 0
Failed Registrations: 0
Dell#
```

Related Commands

show gvrp — displays the GVRP configuration.

show vlan

Display the global VLAN configuration.

Syntax

`show vlan`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell# show vlan
  Codes: * - Default VLAN, G - GVRP VLANs, R - Remote Port
Mirroring VLANs, P -
Primary, C - Community, I - Isolated
Q: U - Untagged, T - Tagged
   x - Dot1x untagged, X - Dot1x tagged
   G - GVRP tagged, M - Vlan-stack, H - VSN tagged
   i - Internal untagged, I - Internal tagged, v - VLT
untagged, V - VLT tagged
     NUM Status Description   Q Ports
```

```
*    1   Active               U Te 3/20
                              U Te 5/20-21

G    10  Active               G Po128(Te 5/49) (dynamically
leanred vlan)
Dell
```

Related Commands

show gvrp statistics — displays the GVRP statistics.

20

Internet Group Management Protocol (IGMP)

The IGMP commands are supported by the Dell Networking Operating System (OS).

IGMP Snooping Commands

The Dell Networking OS supports IGMP Snooping version 2 and 3 on all Dell Networking systems.

Important Points to Remember for IGMP Snooping

- The Dell Networking OS supports version 1, version 2, and version 3 hosts.
- The Dell Networking OS IGMP snooping implementation is based on IP multicast address (not based on Layer 2 multicast mac address) and the IGMP snooping entries are in Layer 3 flow table not in Layer 2 forwarding information base (FIB).
- The Dell Networking OS IGMP snooping implementation is based on draft-ietf-magma-snoop-10.
- IGMP snooping is not enabled by default on the switch.
- A maximum of 1800 groups and 600 virtual local area network (VLAN) are supported.
- IGMP snooping is not supported on a default VLAN interface.
- IGMP snooping is not supported over VLAN-Stack-enabled VLAN interfaces (you must disable IGMP snooping on a VLAN interface before configuring VLAN-Stack-related commands).
- IGMP snooping does not react to Layer 2 topology changes triggered by spanning tree protocol (STP).
- IGMP snooping reacts to Layer 2 topology changes multiple spanning tree protocol (MSTP) triggers by sending a general query on the interface that comes in the FWD state.

Important Points to Remember for IGMP Querier

- The IGMP snooping Querier supports version 2.
- You must configure an IP address to the VLAN interface for IGMP snooping Querier to begin. The IGMP snooping Querier disables itself when a VLAN IP address is cleared, and then it restarts itself when an IP address is reassigned to the VLAN interface.
- When enabled, IGMP snooping Querier does not start if there is a statically configured multicast router interface in the VLAN.
- When enabled, IGMP snooping Querier starts after one query interval in case no IGMP general query (with IP SA lower than its VLAN IP address) is received on any of its VLAN members.
- When enabled, IGMP snooping Querier periodically sends general queries with an IP source address of the VLAN interface. If it receives a general query on any of its VLAN member, it checks the IP source address of the incoming frame.
- If the IP SA in the incoming IGMP general query frame is lower than the IP address of the VLAN interface, the switch disables its IGMP snooping Querier functionality.

- If the IP SA of the incoming IGMP general query is higher than the VLAN IP address, the switch continues to work as an IGMP snooping Querier.

ip igmp access-group

To specify access control for packets, use this feature.

Syntax	`ip igmp access-group access-list` To remove the feature, use the `no ip igmp access-group access-list` command.
Parameters	*access-list* — Enter the name of the extended ACL (16 characters maximum).
Defaults	Not configured
Command Modes	INTERFACE (conf-if-*interface-slot/port*)
Command History	**Version 8.3.16.1** — Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	The access list accepted is an extended ACL. To block IGMP reports from hosts, on a per-interface basis based on the group address and source address that you specify in the access list, use this feature.

ip igmp group-join-limit

To limit the number of IGMP groups that can be joined in a second, use this feature.

Syntax	`ip igmp group-join-limit number`
Parameters	*number* — Enter the number of IGMP groups permitted to join in a second. The range is from 1 to 10000.
Defaults	none
Command Modes	CONFIGURATION (conf-if-*interface-slot/port*)
Command History	**Version 8.3.16.1** — Introduced on the MXL 10/40GbE Switch IO Module.

ip igmp querier-timeout

Change the interval that must pass before a multicast router decides that there is no longer another multicast router that should be the querier.

Syntax `ip igmp querier-timeout` *`seconds`*

To return to the default value, use the `no ip igmp querier-timeout` command.

Parameters

seconds	Enter the number of seconds the router must wait to become the new querier. The range is from 60 to 300. The default is **125 seconds**.

Defaults **125 seconds**

Command Modes INTERFACE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

ip igmp query-interval

Change the transmission frequency of IGMP general queries the Querier sends.

Syntax `ip igmp query-interval` *`seconds`*

To return to the default values, use the `no ip igmp query-interval` command.

Parameters

seconds	Enter the number of seconds between queries sent out. The range is from 1 to 18000. The default is **60 seconds**.

Defaults **60 seconds**

Command Modes INTERFACE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

ip igmp query-max-resp-time

Set the maximum query response time advertised in general queries.

Syntax	`ip igmp query-max-resp-time` *`seconds`* To return to the default values, use the `no ip igmp query-max-resp-time` command.
Parameters	*seconds*: Enter the number of seconds for the maximum response time. The range is from 1 to 25. The default is **10 seconds**.
Defaults	**10 seconds**
Command Modes	INTERFACE
Command History	Version 8.3.16.1: Introduced on the MXL 10/40GbE Switch IO Module.

ip igmp version

Manually set the version of the router to IGMPv2 or IGMPv3.

Syntax	`ip igmp version {2 | 3}`
Parameters	2: Enter the number 2 to set the IGMP version number to IGMPv2. 3: Enter the number 3 to set the IGMP version number to IGMPv3.
Defaults	**2** (that is, IGMPv2)
Command Modes	INTERFACE
Command History	Version 8.3.16.1: Introduced on the MXL 10/40GbE Switch IO Module.

ip igmp snooping enable

Enable IGMP snooping on all or a single VLAN. This command is the master on/off switch to enable IGMP snooping.

Syntax	`ip igmp snooping enable` To disable IGMP snooping, use the `no ip igmp snooping enable` command.

Defaults

Disabled.

Command Modes

- CONFIGURATION
- INTERFACE VLAN

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To enable IGMP snooping, enter this command. When you enable this command from CONFIGURATION mode, IGMP snooping enables on all VLAN interfaces (except the default VLAN).

NOTE: Execute the `no shutdown` command on the VLAN interface for IGMP Snooping to function.

Related Commands

shutdown — (no shutdown) activates an interface.

ip igmp snooping fast-leave

Enable IGMP snooping fast-leave for this VLAN.

Syntax

```
ip igmp snooping fast-leave
```

To disable IGMP snooping fast leave, use the `no igmp snooping fast-leave` command.

Defaults

Not configured.

Command Modes

INTERFACE VLAN — (conf-if-vl-*n*)

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Queriers normally send some queries when a leave message is received prior to deleting a group from the membership database. There may be situations when you require a *fast* deletion of a group. When you enable IGMP fast leave processing, the switch removes an interface from the multicast group as soon as it detects an IGMP version 2 leave message on the interface.

ip igmp snooping flood

This command controls the flooding behavior of unregistered multicast data packets.

Syntax

```
ip igmp snooping flood
```

Defaults	Enabled.
Command Modes	CONFIGURATION
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	When you disable flooding, unregistered multicast data traffic is forwarded to only multicast router ports, both static and dynamic, in a VLAN. If there is no multicast router port in a VLAN, unregistered multicast data traffic is dropped. On the MXL switch, when you configure `no ip igmp snooping flood`, the system forwards the frames on mrouter ports for first 96 IGMP snooping enabled VLANs. For all other VLANs, unregistered multicast packets are dropped.

ip igmp snooping last-member-query-interval

The last member query interval is the maximum response time inserted into Group-Specific queries sent in response to Group-Leave messages.

Syntax	`ip igmp snooping last-member-query-interval` *`milliseconds`* To return to the default value, use the `no ip igmp snooping last-member-query-interval` command.
Parameters	*milliseconds* Enter the interval in milliseconds. The range is from 100 to 65535. The default is **1000 milliseconds**.
Defaults	**1000 milliseconds**
Command Modes	INTERFACE VLAN
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	This last-member-query-interval is also the interval between successive Group-Specific Query messages. To change the last-member-query interval, use this command.

ip igmp snooping mrouter

Statically configure a VLAN member port as a multicast router interface.

Syntax	`ip igmp snooping mrouter interface` *`interface`*

To delete a specific multicast router interface, use the `no igmp snooping mrouter interface` *`interface`* command.

Parameters

interface *interface*	Enter the following keywords and slot/port or number information: • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.

Defaults Not configured.

Command Modes INTERFACE VLAN — (conf-if-vl-*n*)

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information The Dell Networking OS provides the capability of statically configuring the interface to which a multicast router is attached. To configure a static connection to the multicast router, enter the `ip igmp snooping mrouter interface` command in the VLAN context. The interface to the router must be a part of the VLAN where you are entering the command.

ip igmp snooping querier

Enable IGMP querier processing for the VLAN interface.

Syntax

```
ip igmp snooping querier
```

To disable IGMP querier processing for the VLAN interface, use the `no ip igmp snooping querier` command.

Defaults Not configured.

Command Modes INTERFACE VLAN — (conf-if-vl-*n*)

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information This command enables the IGMP switch to send General Queries periodically. This behavior is useful when there is no multicast router present in the VLAN because the multicast traffic is not routed. Assign an IP address to the VLAN interface for the switch to act as a querier for this VLAN.

show ip igmp snooping mrouter

Display multicast router interfaces.

Syntax	`show ip igmp snooping mrouter [vlan *number*]`

Parameters

vlan *number*	Enter the keyword `vlan` then the VLAN number. The range is from 1 to 4094.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show ip igmp snooping mrouter
Interface Router Ports
Vlan 2 Gi 13/3, Po 1
Dell#
```

21

Interfaces

The commands in this chapter are supported by Dell Networking Operating System (OS).

This chapter contains the following sections:

- Basic Interface Commands
- Port Channel Commands

Basic Interface Commands

The following commands are for Physical, Loopback, and Null interfaces.

clear counters

Clear the counters used in the `show interfaces` commands for all virtual router redundancy protocol (VRRP) groups, virtual local area networks (VLANs), and physical interfaces, or selected ones.

Syntax

```
clear counters [interface] [vrrp [{vrid | vrf instance}]|
learning-limit]
```

Parameters

interface	(OPTIONAL) Enter any of the following keywords and slot/port or number to clear counters from a specified interface: • For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383. • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For the management interface on the RPM, enter the keyword `ManagementEthernet` then slot/port information. The slot range is from 0 to 1 and the port range is 0. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a VLAN, enter the keyword `VLAN` then a number from 1 to 4094.
vrrp *vrid*]	(OPTIONAL) Enter the keyword `vrrp` to clear the counters of all VRRP groups. To clear the counters of a specified group, enter a VRID number from 1 to 255.

vrrp [vrf *instance*]	(OPTIONAL) Enter the keyword `vrrp` to clear the counters of all VRRP groups. To clear the counters of VRRP groups in a specified VRF instance, enter the name of the instance (32 characters maximum).
learning-limit	(OPTIONAL) Enter the keywords `learning-limit` to clear unknown source address (SA) drop counters when MAC learning limit is configured on the interface.

Defaults

Without an interface specified, the command clears all interface counters.

Command Modes

EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#clear counters
Clear counters on all interfaces [confirm]
```

Related Commands

mac learning-limit — allows aging of MACs even though a learning-limit is configured or disallow station move on learned MACs.

show interfaces — displays information on the interfaces.

clear dampening

Clear the dampening counters on all the interfaces or just the specified interface.

Syntax

`clear dampening [interface]`

Parameters

interface	(OPTIONAL) Enter any of the following keywords and slot/port or number to clear counters from a specified interface: • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

Defaults

Without an interface specified, the command clears all interface dampening counters.

Command Modes	EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

On the MXL switch, after you enter the `clear counters` command and verify the results with the `show interfaces` command, the line rate is not reset to 0.00%.

Example

```
Dell#clear dampening gigabitethernet 1/2
Clear dampening counters on tengig 1/2 [confirm] y
Dell#
```

Related Commands

show interfaces dampening — displays interface dampening information.

dampening — configures dampening on an interface.

cx4-cable-length

Configure the length of the cable to be connected to the selected CX4 port.

Syntax

```
[no] cx4-cable-length {long | medium | short}
```

Parameters

long | medium | short — Enter the keyword that matches the cable length to be used at the selected port:

- `short` = For 1-meter and 3-meter cable lengths.
- `medium` = For 5-meter cable length.
- `long` = For 10-meter and 15-meter cable lengths.

Defaults

medium

Command Modes

INTERFACE

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

This command only works on ports that the system recognizes as CX4 ports. The figures below shows an attempt to configure an XFP port with the command after inserting a CX4 converter into the port.

For details about using XFP ports with CX4 cables, refer to your MXL switch hardware guide.

Example (Unsuccessful)

```
Dell#show interfaces tengigabitethernet 0/26 | grep "XFP type"

Pluggable media present, XFP type is 10GBASE-CX4

Dell(conf-if-te-0/26)#cx4-cable-length short
% Error: Unsupported command.
Dell(conf-if-te-0/26)#cx4-cable-length medium
% Error: Unsupported command.
Dell(conf-if-te-0/26)#cx4-cable-length long
% Error: Unsupported command.
Dell(conf-if-te-0/26)#
```

Example (Successful)

```
Dell#config
Dell(config)#interface tengigabitethernet 0/52
Dell(conf-if-0/52)#cx4-cable-length long
Dell(conf-if-0/52)#show config
!
interface TenGigabitEthernet 0/51
  no ip address
  cx4-cable-length long
  shutdown
Dell(conf-if-0/52)#exit
Dell(config)#
```

Related Commands

show config – displays the configuration of the selected interface.

dampening

Configure dampening on an interface.

Syntax

`dampening [[[[half-life] [reuse-threshold]] [suppress-threshold]] [max-suppress-time]]`

To disable dampening, use the `no dampening [[[[half-life] [reuse-threshold]] [suppress-threshold]] [max-suppress-time]]` command.

Parameters

half-life	Enter the number of seconds after which the penalty is decreased. The penalty decreases half after the half-life period expires. The range is from 1 to 30 seconds. The default is **5 seconds**.
reuse-threshold	Enter a number as the reuse threshold, the penalty value below which the interface state is changed to “up”. The range is from 1 to 20000. The default is **750**.
suppress-threshold	Enter a number as the suppress threshold, the penalty value above which the interface state is changed to “error disabled”. The range is from 1 to 20000. The default is **2500**.

max-suppress-time	Enter the maximum number for which a route can be suppressed. The default is four times the half-life value. The range is from 1 to 86400. The default is **20 seconds**.

Defaults

Disabled.

Command Modes

INTERFACE (conf-if-)

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

With each flap, The Dell Networking OS penalizes the interface by assigning a penalty (1024) that decays exponentially depending on the configured half-life. After the accumulated penalty exceeds the suppress threshold value, the interface moves to the Error-Disabled state. This interface state is deemed as “down” by all static/dynamic Layer 2 and Layer 3 protocols. The penalty is exponentially decayed based on the half-life timer. After the penalty decays below the reuse threshold, the interface enables. The configured parameters are as follows:

- `suppress-threshold` should be greater than `reuse-threshold`
- `max-suppress-time` should be at least 4 times `half-life`

NOTE: You cannot apply dampening on an interface that is monitoring traffic for other interfaces.

Example

```
Dell(conf-if-gi-3/2)#dampening 20 800 4500 120
Dell(conf-if-gi-3/2)#
```

Related Commands

clear dampening — clears the dampening counters on all the interfaces or just the specified interface.

show interfaces dampening — displays interface dampening information.

description

Assign a descriptive text string to the interface.

Syntax

`description desc_text`

To delete a description, use the `no description` command.

Parameters

desc_text	Enter a text string up to 240 characters long. To use special characters as a part of the description string, you must enclose the whole string in double quotes.

Defaults

none

Command Modes

INTERFACE

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Important Points to Remember:

- Spaces between characters are not preserved after entering this command unless you enclose the entire description in quotation marks (“*`desc_text`*”).
- Entering a text string after the `description` command overwrites any previous text string that you previously configured as the description.
- The `shutdown` and `description` commands are the only commands that you can configure on an interface that is a member of a port-channel.
- Use the `show interfaces description` command to display descriptions configured for each interface.

Related Commands

show interfaces description — displays the description field of the interfaces.

duplex (1000/10000 Interfaces)

Configure duplex mode on any physical interfaces where the speed is set to 1000/10000.

Syntax

```
duplex {half | full}
```

To return to the default setting, use the `no duplex` command.

Parameters

half	Enter the keyword `half` to set the physical interface to transmit only in one direction.
full	Enter the keyword `full` to set the physical interface to transmit in both directions.

Defaults

Not configured.

Command Modes

INTERFACE

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

This command applies to any physical interface with speed set to 1000/10000.

NOTE: Starting with the Dell Networking OS version 7.8.1.0, when you use a copper SFP2 module with catalog number GP-SFP2-1T in the S25P module, you can manually set its speed with the `speed` command. When you set the speed to 10 Mbps or 100 Mbps, you can also execute the `duplex` command.

Related Commands

speed (for 1000/10000/auto interfaces) — sets the speed on the Base-T Ethernet interface.

negotiation auto — enables or disables auto-negotiation on an interface.

flowcontrol

Control how the system responds to and generates 802.3x pause frames on 10G and 40Gig stack units.

Syntax

```
flowcontrol rx {off | on} tx {off | on} threshold
```

Parameters

rx on	Enter the keywords `rx on` to process the received flow control frames on this port. This is the default value for the receive side.
rx off	Enter the keywords `rx off` to ignore the received flow control frames on this port.
tx on	Enter the keywords `tx on` to send control frames from this port to the connected device when a higher rate of traffic is received. This is the default value on the send side.
tx off	Enter the keywords `tx off` so that flow control frames are not sent from this port to the connected device when a higher rate of traffic is received.

Defaults

- `rx off`
- `tx off`

Command Modes

INTERFACE

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The globally assigned 48-bit Multicast address 01-80-C2-00-00-01 is used to send and receive pause frames. To allow full-duplex flow control, stations implementing the pause operation instruct the MAC to enable the reception of frames with a destination address equal to this multicast address.

The pause:

- Starts when *either* the packet pointer or the buffer threshold is met (whichever is met first). When the discard threshold is met, packets are dropped.
- Ends when *both* the packet pointer and the buffer threshold fall below 50% of the threshold settings.

The *discard threshold* defines when the interface starts dropping the packet on the interface. This may be necessary when a connected device does not honor the flow control frame sent by the switch. The discard threshold should be larger than the *buffer threshold* so that the buffer holds at least hold at least three packets.

On 4–port 10G stack units: Changes in the flow-control values may not be reflected automatically in the `show interface` output for 10G interfaces. This is because 10G interfaces do not support auto-negotiation.

Important Points to Remember

- Do not enable `tx pause` when buffer carving is enabled. For information and assistance, consult Dell Networking TAC.
- Asymmetric flow control (`rx on tx off`, or `rx off tx on`) setting for the interface port less than 100 Mb/s speed is not permitted. The following error is returned:

  ```
  Can’t configure Asymmetric flowcontrol when speed <1G,
  config ignored
  ```
- The only configuration applicable to half duplex ports is `rx off tx off`. The following error is returned:

  ```
  Cannot configure Asymmetric flowcontrol when speed <1G,
  config ignored>
  ```
- You cannot configure half duplex when the flow control configuration is on (default is `rx on tx on`). The following error is returned: `Cannot configure half duplex when flowcontrol is on, config ignored`

NOTE: The flow control must be off (`rx off tx off`) before configuring the half duplex.

Example (partial)

```
Dell(conf-if-tengig-0/1)#show config
!
interface TenGigabitEthernet 0/1
no ip address
switchport
no negotiation auto
flowcontrol rx off tx on
no shutdown
...
```

Example (Values)

This Example shows how the Dell Networking OS negotiates the flow control values between two Dell Networking chassis connected back-to-back using 1G copper ports.

```
Configured
```

```
LocRxConf LocTxConf RemoteRxConf RemoteTxConf
off       off        off           off
                     off           on
                     on            off
                     on            on

off       on         off           off
                     off           on
                     on            off
                     on            on

on        off        off           off
                     off           on
                     on            off
                     on            on

on        on         off           off
                     off           on
                     on            off
                     on            on

LocNegRx LocNegTx RemNegRx RemNegTx
off      off     off      off
off      off     off      off
off      off     off      off
off      off     off      off

off      off     off      off
off      off     off      off
off      on      on       off
off      off     off      off

off      off     off      off
on       off     off      on
on       on      on       on
on       on      on       on

off      off      off     off
off      off      off     off
on       on       on      on
on       on       on      on
```

Related Commands

show running-config — displays the flow configuration parameters (non-default values only).

show interfaces — displays the negotiated flow control parameters.

interface

Configure a physical interface on the switch.

Syntax `interface interface`

Parameters

interface	Enter one of the following keywords and slot/port or number information:

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a Fibre Channel interface, enter the keyword `FibreChannel`, then the slot/port information.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

Version 9.4(0.0)	Added the support for interfaces.
Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

You cannot delete a physical interface.

By default, physical interfaces are disabled (`shutdown`) and are in Layer 3 mode. To place an interface in mode, ensure that the interface's configuration does not contain an IP address and enter the `Port Channel Commands` command.

The tunnel interface operates as an ECMP (equal cost multi path) only when the next hop to the tunnel destination is over a physical interface. If you select any other interface as the next hop to the tunnel destination, the tunnel interface does not operate as an ECMP.

Example

```
Dell(conf)#interface tengig 0/0
Dell(conf-if-tengig-0/0)#exit#
```

Related Commands

interface port-channel — configures a port channel.

interface vlan — configures a VLAN.

show interfaces — displays the interface configuration.

interface loopback

Configure a Loopback interface.

Syntax

`interface loopback` *`number`*

To remove a loopback interface, use the `no interface loopback` *`number`* command.

Parameters	*number*	Enter a number as the interface number. The range is from 0 to 16383.
Defaults	Not configured.	
Command Modes	CONFIGURATION	
Command History	Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell(conf)#interface loopback 1655
Dell(conf-if-lo-1655)#
```

Related Commands

interface — configures a physical interface.

interface null — configures a Null interface.

interface port-channel — configures a port channel.

interface vlan — configures a VLAN.

interface ManagementEthernet

Configure the Management port on the system.

Syntax `interface ManagementEthernet slot/port`

Parameters	*slot/port*	Enter the keyword `ManagementEthernet`, then the slot number (0 or 1) and port number zero (0).
Defaults	Not configured.	
Command Modes	CONFIGURATION	
Command History	Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

You cannot delete a Management port.

The Management port is enabled by default (`no shutdown`). To assign an IP address to the Management port, use the `ip address` command.

Example

```
Dell(conf)#interface managementethernet 0/0
Dell(conf-if-ma-0/0)#
```

interface null

Configure a Null interface on the switch.

Syntax `interface null number`

Parameters

number	Enter zero (0) as the Null interface number.

Defaults Not configured; number = **0**

Command Modes CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information You cannot delete the Null interface. The only configuration command possible in a Null interface is `ip unreachables`.

Example

```
Dell(conf)#interface null 0
Dell(conf-if-nu-0)#
```

Related Commands

interface — configures a physical interface.

interface loopback — configures a Loopback interface.

interface port-channel — configures a port channel.

interface vlan — configures a VLAN.

ip unreachables — enables generation of internet control message protocol (ICMP) unreachable messages.

interface range

This command permits configuration of a range of interfaces to which subsequent commands are applied (bulk configuration). Using the `interface range` command, you can enter identical commands for a range of interface.

Syntax `interface range interface, interface,...`

Parameters

interface, interface,...	Enter the keywords `interface range` and one of the interfaces — slot/port, port-channel, or VLAN number. Select the range of interfaces for bulk configuration. You can enter up to six comma-separated ranges. Spaces are not required between the commas. Comma-separated ranges can include VLANs, port-channels, and physical interfaces. Slot/Port information must contain a space before and after the dash. For example, `interface range gigabitethernet 0/1 - 5` is valid; `interface range gigabitethernet 0/1-5` is NOT valid. • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

Defaults none

Command Modes CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

When creating an interface range, interfaces appear in the order they are entered; they are not sorted. The command verifies that interfaces are present (physical) or configured (logical).

Important Points to Remember:

- Bulk configuration is created if at least one interface is valid.
- Non-existing interfaces are excluded from the bulk configuration with a warning message.
- The `interface range` prompt includes interface types with slot/port information for valid interfaces. The prompt allows for a maximum of 32 characters. If the bulk configuration exceeds 32 characters, it is represented by an ellipsis (...).
- When the `interface range` prompt has multiple port ranges, the smaller port range is excluded from the prompt.
- If overlapping port ranges are specified, the port range is extended to the smallest start port and the biggest end port.

Example (Bulk)

```
Dell(conf)#interface range so 2/0-1, te 10/0, gi 3/0, fa 0/0
% Warning: Non-existing ports (not configured) are ignored by
interface-range
```

Example (Multiple Ports)

```
Dell(conf)#interface range gi 2/0 - 23, gi 2/1 - 10
Dell(conf-if-range-gi-2/0-23#
```

Example (Overlapping Ports)

```
Dell(conf)#interface range gi 2/1 - 11, gi 2/1 - 23
Dell(conf-if-range-gi-2/1-23#
```

Usage Information

Only VLAN and port-channel interfaces created using the `interface vlan` and `interface port-channel` commands can be used in the `interface range` command.

Use the `show running-config` command to display the VLAN and port-channel interfaces. VLAN or port-channel interfaces that are not displayed in the `show running-config` command cannot be used with the bulk configuration feature of the `interface range` command. You cannot create virtual interfaces (VLAN, Port-channel) using the `interface range` command.

NOTE: If a range has VLAN, physical, port-channel, and SONET interfaces, only commands related to physical interfaces can be bulk configured. To configure commands specific to VLAN or port-channel, only those respective interfaces should be configured in a particular range.

Example (Single Range)

This example shows a single range bulk configuration.

```
Dell(config)# interface range gigabitethernet 5/1 - 23
Dell(config-if-range)# no shutdown
Dell(config-if-range)#
```

Example (Multiple Range)

This example shows how to use commas to add different interface types to the range enabling all Gigabit Ethernet interfaces in the range 5/1 to 5/23 and both Ten-Gigabit Ethernet interfaces 1/1 and 1/2.

```
Dell(config-if)# interface range gigabitethernet5/1-23,
tengigabitethernet1/1-2
Dell(config-if-range)# no shutdown
Dell(config-if-range)#
```

Example (Multiple Range)

This example shows how to use commas to add SONET, VLAN, and port-channel interfaces to the range.

```
Dell(config-if)# interface range gigabitethernet5/1-23,
tengigabitethernet1/1-2,
Vlan 2–100, Port 1–25
Dell(config-if-range)# no shutdown
Dell(config-if-range)#
```

Related Commands

interface port-channel — configures a port channel group.

[interface vlan](#) — configures a VLAN interface.

[show config (from INTERFACE RANGE mode)](#) — shows the bulk configuration interfaces.

[show range](#) — shows the bulk configuration ranges.

interface range macro (define)

Defines a macro for an interface range and then saves the macro in the running configuration.

Syntax `define interface range macro` *`name interface , interface , ...`*

Parameters

name	Enter up to 16 characters for the macro name.
interface, interface,...	Enter the keywords `interface range` and one of the interfaces — slot/port, port-channel, or VLAN number. Select the range of interfaces for bulk configuration. You can enter up to six comma-separated ranges. Spaces are not required between the commas. Comma-separated ranges can include VLANs, port-channels, and physical interfaces. Slot/Port information must contain a space before and after the dash. For example, `interface range gigabitethernet 0/1 - 5` is valid; `interface range gigabitethernet 0/1-5` is NOT valid. • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

Defaults none

Command Modes CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example (Single Range)	This example shows how to define an interface range macro named test. Execute the `show running-config` command to display the macro definition.

```
Dell(config)# define interface-range test
tengigabitethernet0/0-3,
gigabitethernet 5/0-47, gigabitethernet 13/0-89

Dell# show running-config | grep define
define interface-range test tengigabitethernet0/0-3,
gigabitethernet5/0-47,
gigabitethernet 13/0 - 89
Dell(config)#interface range macro test
Dell(config-if-range-te-0/0-3,gi-5/0-47,gi-13/0-89)#
```

Related Commands	interface range – configures a range of command (bulk configuration) interface range macro name – runs an interface range macro.

interface range macro name

Run the interface-range macro to automatically configure the pre-defined range of interfaces.

Syntax	`interface range macro name`
Parameters	*name* — Enter the name of an existing macro.
Defaults	none
Command Modes	CONFIGURATION
Command History	**Version 9.2(0.0)** — Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only. **Version 8.3.16.1** — Introduced on the MXL 10/40GbE Switch IO Module.
Example (Single Range)	This example shows the macro named *test* that was defined earlier.

```
Dell(config)#interface range macro test
Dell(config-if-range-te-0/0-3,gi-5/0-47,gi-13/0-89)#
```

Related Commands	interface range — configures a range of command (bulk configuration). interface range macro (define) — defines a macro for an interface range (bulk configuration).

interface vlan

Configure a VLAN. You can configure up to 4096 VLANs.

Syntax

`interface vlan vlan-id`

To delete a VLAN, use the `no interface vlan vlan-id` command.

Parameters

vlan-id	Enter a number as the VLAN Identifier. The range is from 1 to 4096.

Defaults

Not configured, except for the Default VLAN, which is configured as VLAN 1.

Command Modes

CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

For more information about VLANs and the commands to configure them, refer to the Virtual LAN (VLAN) Commands.

FTP, TFTP, and SNMP operations are not supported on a VLAN. MAC/IP ACLs are not supported.

Example

```
Dell(conf)#int vlan 3
Dell(conf-if-vl-3)#
```

Related Commands

interface — configures a physical interface.

interface port-channel — configures a port channel group.

intf-type cr4 autoneg

Set the interface type as CR4 with auto-negotiation enabled.

Syntax

`intf-type cr4 autoneg`

If you configure `intf-type cr4 autoneg`, use the `no intf-type cr4 autoneg` command to set the interface type as cr4 with autonegotiation disabled.

Defaults

Not configured

Command Modes

CONFIGURATION

Command History	**Version 9.2(0.0)**	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

If you configure `interface type` as CR4 with auto-negotiation enabled, also configure CR4 with auto-negotiation. Many DAC cable link issues are resolved by setting the interface type as CR4.

Related Commands

interface — configures a physical interface.

interface port-channel — configures a port channel group.

keepalive

Send keepalive packets periodically to keep an interface alive when it is not transmitting data.

Syntax

`keepalive [seconds]`

To stop sending keepalive packets, use the `no keepalive` command.

Parameters

seconds	(OPTIONAL) For interfaces with PPP encapsulation enabled, enter the number of seconds between keepalive packets. The range is from 0 to 23767. The default is **10 seconds**.

Defaults

Enabled.

Command Modes

INTERFACE

Command History	**Version 9.2(0.0)**	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

When you configure `keepalive`, the system sends a self-addressed packet out of the configured interface to verify that the far end of a WAN link is up. When you configure `no keepalive`, the system does not send keepalive packets and so the local end of a WAN link remains up even if the remote end is down.

monitor interface

Monitor counters on a single interface or all interfaces on a line card. The screen is refreshed every five seconds and the CLI prompt disappears.

Syntax

`monitor interface [`*`interface`*`]`

To disable monitoring and return to the CLI prompt, press the `q` key.

Parameters

interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For the management port, enter the keyword `managementethernet` then the slot (0 or 1) and the port (0). • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

In the Example, the delta column displays changes since the last screen refresh.

The following are the `monitor` command menu options.

Key	Description
systest-3	Displays the host name assigned to the system.
monitor time	Displays the amount of time since the `monitor interface` command was entered.
time	Displays the amount of time the chassis is up (since last reboot).
m	Change the view from a single interface to all interfaces on the line card or visa-versa.
c	Refresh the view.
b	Change the counters displayed from Packets on the interface to Bytes.
r	Change the [delta] column from change in the number of packets/bytes in the last interval to rate per second.

Key	Description
l	Change the view to the next interface on the line card, or if in line card mode, the next line card in the chassis.
a	Change the view to the previous interface on the line card, or if in line card mode, the previous line card in the chassis.
T	Increase the screen refresh rate.
t	Decrease the screen refresh rate.
q	Return to the CLI prompt.

Example (Single Interface)

```
systest-3 Monitor time: 00:00:06 Refresh Intvl.: 2s Time:
03:26:26

Interface: Gi 0/3, Enabled, Link is Up, Linespeed is 1000 Mbit

Traffic statistics:    Current    Rate      Delta
       Input bytes:    9069828  43 Bps      86
      Output bytes:  606915800  43 Bps      86
     Input packets:      54001   0 pps       1
    Output packets:    9401589   0 pps       1
       64B packets:         67   0 pps       0
  Over 64B packets:      49166   0 pps       1
 Over 127B packets:        350   0 pps       0
 Over 255B packets:       1351   0 pps       0
 Over 511B packets:        286   0 pps       0
Over 1023B packets:       2781   0 pps       0
  Error statistics:
   Input underruns:          0   0 pps       0
      Input giants:          0   0 pps       0
   Input throttles:          0   0 pps       0
         Input CRC:          0   0 pps       0
 Input IP checksum:          0   0 pps       0
     Input overrun:          0   0 pps       0
  Output underruns:          0   0 pps       0
  Output throttles:          0   0 pps       0

  m - Change mode               c - Clear screen
  l - Page up                   a - Page down
  T - Increase refresh interval  t - Decrease refresh interval
  q - Quit
```

mtu

Set the link maximum transmission unit (MTU) (frame size) for an Ethernet interface.

Syntax

`mtu value`

To return to the default MTU value, use the `no mtu` command.

Parameters

value	Enter a maximum frame size in bytes. The range is from 594 to 9252. MXL Switch Range is from 594 to 12000. The default is **1554**.

Defaults	**1554**
Command Modes	INTERFACE
Command History	

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

If the packet includes a Layer 2 header, the difference between the link MTU and IP MTU (`ip mtu` command) must be enough bytes to include the Layer 2 header.

- The IP MTU is adjusted automatically when you configure the Layer 2 MTU with the `mtu` command.

When you enter the `no mtu` command, The Dell Networking OS reduces the IP MTU value to 1536 bytes.

Link MTU and IP MTU considerations for port channels and VLANs are as follows.

port channels:

- All members must have the same link MTU value and the same IP MTU value.
- The port channel link MTU and IP MTU must be less than or equal to the link MTU and IP MTU values configured on the channel members. For example, if the members have a link MTU of 2100 and an IP MTU 2000, the port channel's MTU values cannot be higher than 2100 for link MTU or 2000 bytes for IP MTU.

VLANs:

- All members of a VLAN must have same IP MTU value.
- Members can have different Link MTU values. Tagged members must have a link MTU 4 bytes higher than untagged members to account for the packet tag.
- The VLAN link MTU and IP MTU must be less than or equal to the link MTU and IP MTU values configured on the VLAN members. For example, the VLAN contains tagged members with Link MTU of 1522 and IP MTU of 1500 and untagged members with Link MTU of 1518 and IP MTU of 1500. The VLAN's Link MTU cannot be higher than 1518 bytes and its IP MTU cannot be higher than 1500 bytes.

The following shows the difference between Link MTU and IP MTU.

Layer 2 Overhead	Link MTU and IP MTU Delta
Ethernet (untagged)	18 bytes
VLAN Tag	22 bytes
Untagged Packet with VLAN-Stack Header	22 bytes

Layer 2 Overhead	Link MTU and IP MTU Delta
Tagged Packet with VLAN-Stack Header	26 bytes

negotiation auto

Enable auto-negotiation on an interface.

Syntax

`negotiation auto`

To disable auto-negotiation, use the `no negotiation auto` command.

Defaults

Enabled.

Command Modes

INTERFACE

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The `no negotiation auto` command is only available if you first manually set the speed of a port to **10Mbits** or **100Mbits**.

The `negotiation auto` command provides a `mode` option for configuring an individual port to forced-master/forced slave after you enable auto-negotiation.

If you do not use the `mode` option, the default setting is **slave**. If you do not configure forced-master or forced-slave on a port, the port negotiates to either a master or a slave state. Port status is one of the following:

- Forced-master
- Force-slave
- Master
- Slave
- Auto-neg Error — typically indicates that both ends of the node are configured with forced-master or forced-slave.

⚠ **CAUTION: Ensure that one end of your node is configured as forced-master and one is configured as forced-slave. If both are configured the same (that is, forced-master or forced-slave), the `show interfaces` command flaps between an auto-neg-error and forced-master/slave states.**

You can display master/slave settings with the `show interfaces` command.

Example (Master/Slave)

```
Dell(conf)# int tengig 0/0
Dell(conf-if)#neg auto
Dell(conf-if-autoneg)# ?

end         Exit from configuration mode
exit        Exit from autoneg configuration mode
mode        Specify autoneg mode
no          Negate a command or set its defaults
show        Show autoneg configuration information
Dell(conf-if-autoneg)#mode ?
forced-master Force port to master mode
forced-slave Force port to slave mode
Dell(conf-if-autoneg)#
```

Example (Master/Slave, partial)

```
Dell#show interfaces configured
TenGigabitEthernet 13/18 is up, line protocol is up
Hardware is Dell Force10Eth, address is 00:01:e8:05:f7:fc
   Current address is 00:01:e8:05:f7:fc
Interface index is 474791997
Internet address is 1.1.1.1/24
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed 1000 Mbit, Mode full duplex, Master
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interfaces" counters 00:12:42
Queueing strategy: fifo
Input Statistics:
...
```

User Information

Both sides of the link must have auto-negotiation enabled or disabled for the link to come up.

The following details the possible speed and auto-negotiation combinations for a line between two 10/100/1000 Base-T Ethernet interfaces.

Port 0

- auto-negotiation enabled* speed 1000 or auto
- auto-negotiation enabled speed 100
- auto-negotiation disabled speed 100
- auto-negotiation disabled speed 100
- auto-negotiation enabled* speed 1000 or auto

Port 1

- auto-negotiation enabled* speed 1000 or auto
- auto-negotiation enabled speed 100
- auto-negotiation disabled speed 100
- auto-negotiation enabled speed 100
- auto-negotiation disabled speed 100

Link Status Between Port 1 and Port 2

- Up at 1000 Mb/s
- Up at 100 Mb/s

- Up at 100 Mb/s
- Down
- Down

* You cannot disable auto-negotiation when the speed is set to 1000 or auto.

Related Commands	speed (for 1000/10000 interfaces) — sets the link speed to 1000, 10000, or auto-negotiate the speed.

portmode hybrid

To accept *both* tagged and untagged frames, set a physical port or port-channel. A port configured this way is identified as a hybrid port in report displays.

Syntax

`portmode hybrid`

To return a port to accept *either* tagged or untagged frames (non-hybrid), use the `no portmode hybrid` command.

Defaults

non-hybrid

Command Modes

INTERFACE (conf-if-*interface-slot/port*)

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `interface` command shown in the following example. This example sets a port as hybrid, makes the port a tagged member of VLAN 20, and an untagged member of VLAN 10, which becomes the native VLAN of the port. The port now accepts:

- untagged frames and classify them as VLAN 10 frames
- VLAN 20 tagged frames

The following describes the `do show interfaces` command shown in the following example. This example shows output with “Hybrid” as the newly added value for 802.1QTagged. The options for this field are:

- True — port is tagged
- False — port is untagged
- Hybrid — port accepts both tagged and untagged frames

The following describes the `interface vlan` command shown in the following example. This example shows unconfiguration of the hybrid port using the `no portmode hybrid` command.

NOTE: Remove all other configurations on the port before you can remove the hybrid configuration from the port.

Example

```
Dell(conf)#interface tengig 0/20
Dell(conf-if-te-0/20)#no shut
Dell(conf-if-te-0/20)#portmode hybrid
Dell(conf-if-te-0/20)#sw
Dell(conf-if-te-0/20)#int vlan 10
Dell(conf-if-vl-10)#tag tengig 0/20
Dell(conf-if-vl-10)#int vlan 20
Dell(conf-if-vl-20)#untag tengig 0/20
Dell(conf-if-vl-20)#
```

Example (tagged hybrid)

```
Dell(conf)#interface tengig 0/20
Dell(conf-if-te-0/20)#no shut
Dell(conf-if-te-0/20)#portmode hybrid
Dell(conf-if-te-0/20#sw
Dell(conf-if-te-0/20)#int vlan 10
Dell(conf-if-vl-10)#int tengig 0/20
Dell(conf-if-vl-20)# untag tengig 0/20

Dell  (conf-if-vl-20)#

Dell(conf)#do show interfaces switchport tengigabitethernet
3/20

Codes: U - Untagged, T - Tagged
       x - Dot1x untagged, X - Dot1x tagged
       G - GVRP tagged, M - Trunk, H - VSN tagged
       i - Internal untagged, I - Internal tagged, v - VLT
untagged,
       V - VLT tagged

Name: TenGigabitEthernet 3/20

802.1QTagged: Hybrid
Vlan membership:
Q   Vlans
U   20
T   10

Native VlanId: 20.

Dell(conf)#
```

Example (unconfigure the hybrid port)

```
Dell(conf-if-vl-20)#interface vlan 10
Dell(conf-if-vl-10)#no untagged tengig 0/20
Dell(conf-if-vl-10)#interface vlan 20
Dell(conf-if-vl-20)#no tagged tengig 0/20
Dell(conf-if-vl-20)#interface tengig 0/20
Dell(conf-if-te-0/20)#no portmode hybrid
Dell(conf-if-vl-20)#
```

Related Commands

show interfaces switchport — displays the configuration of switchport (Layer 2) interfaces on the switch.

vlan-stack trunk — specifies an interface as a trunk port to the Stackable VLAN network.

rate-interval

Configure the traffic sampling interval on the selected interface.

Syntax `rate-interval seconds`

Parameters

seconds	Enter the number of seconds for which to collect traffic data. The range is from 5 to 299 seconds.

NOTE: For 0 to 5 seconds, polling occurs every 5 seconds. For 6 to 10 seconds, polling occurs every 10 seconds. For any other value, polling occurs every 15 seconds.

Defaults **299 seconds**

Command Modes INTERFACE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information The output of the `show interfaces` command displays the configured rate interval, along with the collected traffic data.

Related Commands show interfaces — displays information on physical and virtual interfaces.

show config

Display the interface configuration.

Syntax `show config`

Command Modes INTERFACE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell(conf-if)#show conf
!
interface GigabitEthernet 1/7
  no ip address
  switchport
  no shutdown
Dell(conf-if)#
```

show config (from INTERFACE RANGE mode)

Display the bulk configured interfaces (`interface range`).

Syntax `show config`

Command Modes CONFIGURATION INTERFACE (conf-if-range)

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell(conf)#interface range gigabitethernet 1/1 - 2
Dell(conf-if-range-gi-1/1-2)#show config
!
interface GigabitEthernet 1/1
  no ip address
  switchport
  no shutdown
!
interface GigabitEthernet 1/2
  no ip address
  switchport
  no shutdown
Dell(conf-if-range-gi-1/1-2)#
```

show interfaces

Display information on a specific physical interface or virtual interface.

Syntax `show interfaces` *`interface`*

Parameters

interface Enter one of the following keywords and slot/port or number information:

- For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383.
- For a management interface, enter the keyword `ManagementEthernet` then the slot/port information. The slot range is 0 to 1 and the port range is 0.
- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is 1 to 128.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

Command Modes	- EXEC - EXEC Privilege
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Starting with Dell Networking OS Release 9.3(0.0), you can also view the configuration of 40-Gigabit Ethernet interfaces by using the `fortyGigE` keyword with the `show interface interface-type brief` command. For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information to indicate the interface.

Use the `show interfaces` command for details on a specific interface. Use the `show interfaces stack-unit` command for details on all interfaces on the designated stack unit.

On the MXL switch, the `show interface` output displays incorrect rate information details over time for link monitoring when the rate-interval is configured for 5 seconds. Dell Networking OS recommends using higher rate-intervals, such as 15 to 299 seconds, to minimize the errors seen.

NOTE: In the CLI output, the power value is rounded to a 3-digit value. For receive/transmit power that is less than 0.000, an `snmp query` returns the corresponding dbm value even though the CLI displays as 0.000.

NOTE: After the counters are cleared, the line-rate continues to increase until it reaches the maximum line rate. When the maximum line rate is reached, there is no change in the line-rate.

User Information

The following table describes the `show interfaces` command shown in the 10G (TeraScale) Example below.

Line	Description
TenGigabitEthernet 2/0...	Interface type, slot/port, and administrative and line protocol status.
Hardware is...	Interface hardware information, assigned MAC address, and current address.
Interface index...	Displays the interface index number used by SNMP to identify the interface.
Internet address...	States whether an IP address is assigned to the interface. If an IP address is assigned, that address is displayed.
MTU 1554...	Displays link and IP MTU information.
LineSpeed	Displays the interface’s line speed, duplex mode, and Slave.
ARP type:...	Displays the ARP type and the ARP timeout value for the interface.

Line	Description
Last clearing...	Displays the time when the `show interfaces` counters where cleared.
Queuing strategy...	States the packet queuing strategy. FIFO means first in first out.
Input Statistics:	Displays all the input statistics including: • Number of packets and bytes into the interface • Number of packets with VLAN tagged headers • Packet size and the number of those packets inbound to the interface • Number of Multicast and Broadcast packets: – Multicasts = number of MAC multicast packets – Broadcasts = number of MAC broadcast packets • Number of runts, giants, and throttles packets: – runts = number of packets that are less than 64B – giants = packets that are greater than the MTU size – throttles = packets containing PAUSE frames • Number of CRC, overrun, and discarded packets: – CRC = packets with CRC/FCS errors – overrun = number of packets discarded due to FIFO overrun conditions – discarded = the sum of runts, giants, CRC, and overrun packets discarded without any processing
Output Statistics:	Displays output statistics sent out of the interface including: • Number of packets, bytes, and underruns out of the interface • Packet size and the number of those packets outbound to the interface • Number of Multicast, Broadcast, and Unicast packets: – Multicasts = number of MAC multicast packets – Broadcasts = number of MAC broadcast packets – Unicasts = number of MAC unicast packets • Number of VLANs, throttles, discards, and collisions:: – Vlans = number of VLAN tagged packets – throttles = packets containing PAUSE frames – discarded = number of packets discarded without any processing – collisions = number of packet collisions – wred=count both packets discarded in the MAC and in the hardware-based queues

Line	Description
Rate information...	Estimate of the input and output traffic rate over a designated interval (30 to 299 seconds). Traffic rate is displayed in bits, packets per second, and percent of line rate.
Time since...	Elapsed time since the last interface status change (hh:mm:ss format).

Example (10G port)

```
Dell#show interfaces tengigabitethernet 2/0
TenGigabitEthernet 2/0 is up, line protocol is up
Hardware is Dell Force10Eth, address is 00:01:e8:05:f7:3a
Interface index is 100990998
Internet address is 213.121.22.45/28
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed 10000 Mbit
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interfaces" counters 02:31:45
Queueing strategy: fifo
Input Statistics:
    0 packets, 0 bytes
    Input 0 IP Packets, 0 Vlans 0 MPLS
    0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
    0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-
byte pkts
    0 symbol errors, 0 runts, 0 giants, 0 throttles
    0 CRC, 0 IP Checksum, 0 overrun, 0 discarded
Output Statistics:
    1 packets, 64 bytes, 0 underruns
    0 Multicasts, 2 Broadcasts, 0 Unicasts
    0 IP Packets, 0 Vlans, 0 MPLS
    0 throttles, 0 discarded
Rate info (interval 299 seconds):
    Input 00.00 Mbits/sec,     0 packets/sec, 0.00% of line-
rate
    Output 00.00 Mbits/sec,    0 packets/sec, 0.00% of line-
rate
Time since last interface status change: 00:00:27
```

Usage Information

The interface counter "over 1023-byte pkts" does not increment for packets in the range 9216 > x < 1023.

The Management port is enabled by default (`no shutdown`). If necessary, use the `ip address` command to assign an IP address to the Management port.

Example (1G SFP)

```
Dell#show interfaces tengigabitethernet 0/44
TenGigabitEthernet 0/44 is up, line protocol is up
Hardware is DellForce10Eth, address is 00:01:e8:43:00:01
    Current address is 00:01:e8:43:00:01
Port is present
Pluggable media present, SFP+ type is 10GBASE-SR
    Medium is MultiRate, Wavelength is 850nm
    SFP+ receive power reading is -3.6041dBm
Interface index is 45420801
Internet address is not set
Mode of IP Address Assignment : NONE
DHCP Client-ID :tenG1730001e8430001
MTU 1554 bytes, IP MTU 1500 bytes
```

```
LineSpeed 10000 Mbit
Flowcontrol rx off tx off
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 21:14:32
Queueing strategy: fifo
Input Statistics:
    94322888 packets, 6036664832 bytes
    94322888 64-byte pkts, 0 over 64-byte pkts, 0 over 127-
byte pkts
    0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-
byte pkts
    0 Multicasts, 94322888 Broadcasts
    0 runts, 0 giants, 0 throttles
    0 CRC, 0 overrun, 0 discarded
Output Statistics:
    180384 packets, 11926850 bytes, 0 underruns
    172622 64-byte pkts, 7762 over 64-byte pkts, 0 over 127-
byte pkts
    0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-
byte pkts
    7762 Multicasts, 87726 Broadcasts, 84896 Unicasts
    0 throttles, 0 discarded, 0 collisions
Rate info (interval 299 seconds):
    Input 00.00 Mbits/sec, 0 packets/sec, 0.00% of line-rate
    Output 00.00 Mbits/sec, 0 packets/sec, 0.00% of line-rate
Time since last interface status change: 21:13:36
Dell#
```

Example (ManagementEthernet)

```
Dell#show interface managementethernet ?
0/0 Management Ethernet interface number
Dell#show interface managementethernet 0/0
ManagementEthernet 0/0 is up, line protocol is up
Hardware is DellForce10Eth, address is 00:1e:c9:f1:00:05
    Current address is 00:1e:c9:f1:00:05
Pluggable media not present
Interface index is 235159752
Internet address is 10.11.209.87/16
Mode of IP Address Assignment : MANUAL
DHCP Client-ID: mgmt001ec9f10005
Virtual-IP is not set
Virtual-IP IPv6 address is not set
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed 100 Mbit, Mode full duplex
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 5d4h57m
Queueing strategy: fifo
    Input 3448753 packets, 950008323 bytes, 3442163 multicast
    Received 0 errors, 0 discarded
    Output 4627 packets, 814226 bytes, 0 multicast
   Output 0 errors, 0 invalid protocol
```

Related Commands

show interfaces configured — displays any interface with a non-default configuration.

show interfaces stack-unit — displays information on all interfaces on a specific stack unit.

strict-priority unicast — displays information of either rate limiting or rate policing on the interface.

show interfaces switchport — displays Layer 2 information about the interfaces.

show inventory — displays the MXL switch type, components (including media), Dell Networking OS version including hardware identification numbers, and configured protocols.

show ip interface — displays Layer 3 information about the interfaces.

show memory — displays the stack unit(s) status.

show range — displays all interfaces configured using the interface range command.

show interfaces configured

Display any interface with a non-default configuration.

Syntax

```
show interfaces configured
```

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show interfaces configured
GigabitEthernet 13/18 is up, line protocol is up
Hardware is Force10Eth, address is 00:01:e8:05:f7:fc
  Current address is 00:01:e8:05:f7:fc
Interface index is 474791997
Internet address is 1.1.1.1/24
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed 1000 Mbit, Mode full duplex, Master
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interfaces" counters 00:12:42
Queueing strategy: fifo
Input Statistics:
  10 packets, 10000 bytes
  0 Vlans
  0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
  0 over 255-byte pkts, 10 over 511-byte pkts, 0 over 1023-
byte pkts
  0 Multicasts, 0 Broadcasts
  0 runts, 0 giants, 0 throttles
  0 CRC, 0 overrun, 0 discarded
Output Statistics:
  1 packets, 64 bytes, 0 underruns
  1 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
  0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte
pkts
  0 Multicasts, 1 Broadcasts, 0 Unicasts
  0 Vlans, 0 throttles, 0 discarded, 0 collisions
Rate info (interval 299 seconds):
  Input 00.00 Mbits/sec, 0 packets/sec, 0.00% of line-rate
  Output 00.00 Mbits/sec, 0 packets/sec, 0.00% of line-rate
Time since last interface status change: 00:04:59
Dell#
```

Related Commands

show interfaces — displays information on a specific physical interface or virtual interface.

show interfaces dampening

Display interface dampening information.

Syntax

`show interfaces dampening [[`*`interface`*`] [summary] [detail]]`

Parameters

interface	(Optional) Enter one of the following keywords and slot/port or number information: • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
summary	(OPTIONAL) Enter the keyword `summary` to display the current summary of dampening data, including the number of interfaces configured and the number of interfaces suppressed, if any.
detail	(OPTIONAL) Enter the keyword `detail` to display detailed interface dampening data.

Defaults

none

Command Modes

EXEC

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show interfaces dampening
Interface Supp   Flaps Penalty Half-Life Reuse Suppress Max-Sup
          State
Gi 3/2    Up     0     0        20       800   4500     120
Gi 3/10   Up     0     0        5        750   2500     20
Dell#
```

Related Commands

dampening— configures dampening on an interface.

show interfaces — displays information on a specific physical interface or virtual interface.

show interfaces configured — displays any interface with a non-default configuration.

show interfaces description

Display the descriptions configured on the interface.

Syntax `show interfaces [interface] description`

Parameters

interface	(Optional) Enter one of the following keywords and slot/port or number information: • For Loopback interfaces, enter the keyword `loopback` then a number from 0 to 16383. • For the management interface on the RPM, enter the keyword `ManagementEthernet` then the slot/port information. The slot range is 0-0 and the port range is 0. • For the Null interface, enter the keywords `null 0`. • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For VLAN interfaces, enter the keyword `vlan` then a number from 1 to 4094.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show interfaces description` command shown in the Example below.

Field	Description
Interface	Displays the type of interface and associated slot and port number.
OK?	Indicates if the hardware is functioning properly.
Status	States whether the interface is enabled (up) or disabled (administratively down).
Protocol	States whether IP is enabled (up) or disabled (down) on the interface.

Field	Description
Description	Displays the description (if any) manually configured for the interface.

Example

```
Dell#show interface description
Interface                OK Status      Protocol   Description
TenGigabitEthernet 0/1   NO admin down  down
TenGigabitEthernet 0/2   NO admin down  down
TenGigabitEthernet 0/3   NO admin down  down
TenGigabitEthernet 0/4   NO admin down  down
TenGigabitEthernet 0/5   NO admin down  down
TenGigabitEthernet 0/6   NO admin down  down
TenGigabitEthernet 0/7   NO        up   down
TenGigabitEthernet 0/8   YES       up   up
TenGigabitEthernet 0/9   NO admin down  down
TenGigabitEthernet 0/10  NO admin down  down
TenGigabitEthernet 0/11  NO admin down  down
TenGigabitEthernet 0/12  NO admin down  down
TenGigabitEthernet 0/13  NO admin down  down
TenGigabitEthernet 0/14  NO admin down  down
TenGigabitEthernet 0/15  NO admin down  down
TenGigabitEthernet 0/16  YES       up   up
TenGigabitEthernet 0/17  NO admin down  down
TenGigabitEthernet 0/18  NO admin down  down
TenGigabitEthernet 0/19  NO admin down  down
TenGigabitEthernet 0/20  NO admin down  down
TenGigabitEthernet 0/21  NO admin down  down
```

Related Commands

show interfaces – displays information on a specific physical interface or virtual interface.

show interfaces stack-unit

Display information on all interfaces on a specific MXL switch stack member.

Syntax

`show interfaces stack-unit unit-number`

Parameters

unit-number	Enter the stack member number. The range is from 0 to 5.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show interfaces stack-unit 0
TenGigabitEthernet 0/1 is down, line protocol is down
Hardware is DellForce10Eth, address is 00:1e:c9:f1:00:05
    Current address is 00:1e:c9:f1:00:05
Server Port AdminState is Down
Pluggable media not present
```

```
Interface index is 34148609
Internet address is not set
Mode of IP Address Assignment : NONE
DHCP Client-ID :tenG130001ec9f10005
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed auto
Flowcontrol rx off tx off
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 5d5h24m
Queueing strategy: fifo
Input Statistics:
    0 packets, 0 bytes
    0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
    0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-
byte pkts
    0 Multicasts, 0 Broadcasts
    0 runts, 0 giants, 0 throttles
    0 CRC, 0 overrun, 0 discarded
Output Statistics:
    0 packets, 0 bytes, 0 underruns
    0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
    0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-
byte pkts
    0 Multicasts, 0 Broadcasts, 0 Unicasts
    0 throttles, 0 discarded, 0 collisions
Rate info (interval 299 seconds):
    Input 00.00 Mbits/sec,     0 packets/sec, 0.00% of line-
rate
    Output 00.00 Mbits/sec,    0 packets/sec, 0.00% of line-
rate
Time since last interface status change: 5d5h23m
!-------------output truncated ----------------!
```

Related Commands

show hardware stack-unit — displays data plane and management plane input/output statistics.

show interfaces — displays information on a specific physical interface or virtual interface.

show interfaces status

Display a summary of interface information or specify a stack unit and interface to display status information for that specific interface only.

Syntax

`show interfaces [interface stack-unit unit-number] status`

Parameters

interface (OPTIONAL) Enter one of the following keywords and slot/port or number information:

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show interface status
Port  Description Status Speed  Duplex Vlan
Te 0/1            Down   Auto     Auto --
Te 0/2            Down   Auto     Auto --
Te 0/3            Down   Auto     Auto --
Te 0/4            Down   Auto     Auto --
Te 0/5            Down   Auto     Auto --
Te 0/6            Down   Auto     Auto --
Te 0/7            Down   Auto     Auto --
Te 0/8            Up     10000 Mbit Full --
Te 0/9            Down   Auto     Auto --
Te 0/10           Down   Auto     Auto --
Te 0/11           Down   Auto     Auto --
Te 0/12           Down   Auto     Auto --
Te 0/13           Down   Auto     Auto --
Te 0/14           Down   Auto     Auto --
Te 0/15           Down   Auto     Auto --
Te 0/16           Up     10000 Mbit Full --
Dell#
```

Related Commands

show interfaces — displays information on a specific physical interface or virtual interface.

show interfaces switchport

Display only virtual and physical interfaces in Layer 2 mode. This command displays the Layer 2 mode interfaces' IEEE 802.1Q tag status and VLAN membership.

Syntax `show interfaces switchport [interface | stack-unit unit-id ]`

Parameters

interface

(OPTIONAL) Enter one of the following keywords and slot/port or number information:

- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- Enter the keyword `backup` to view the backup interface for this interface.

stack-unit *unit-id*	(OPTIONAL) Enter the keywords `stack-unit` then the stack member number. The range is from 0 to 5.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show interfaces switchport` command for the following example.

Items	Description
Name	Displays the interface's type, slot, and port number.
802.1QTagged	Displays whether if the VLAN tagged ("True"), untagged ("False"), or hybrid ("Hybrid"), which supports both untagged and tagged VLANs by port 13/0.
Vlan membership	Lists the VLANs to which the interface is a member. Starting with the Dell Networking OS version 7.6.1, this field can display native VLAN membership by port 13/0.

Example

```
Dell#show interfaces switchport
Codes: U - Untagged, T - Tagged
       x - Dot1x untagged, X - Dot1x tagged
       G - GVRP tagged, M - Trunk, H - VSN tagged
       i - Internal untagged, I - Internal tagged, v - VLT
untagged, V - VLT
tagged

Name: TenGigabitEthernet 3/20
802.1QTagged: Hybrid
Vlan membership:
Q    Vlans
U    20
T    10
Native VlanId:    20.
Name: TenGigabitEthernet 5/20
802.1QTagged: False
Vlan membership:
Q    Vlans
U    1

Name: TenGigabitEthernet 5/21
802.1QTagged: False
Vlan membership:
Q    Vlans
U    1

Name: TenGigabitEthernet 5/49 (Port-channel 128)
802.1QTagged: True
Vlan membership:
Q    Vlans
G    10

Name: Port-channel 128
```

```
802.1QTagged: True
Vlan membership:
Q    Vlans
Dell#
```

Related Commands

interface — configures a physical interface on the switch.

show ip interface — displays Layer 3 information about the interfaces.

show interfaces — displays information on a specific physical interface or virtual interface.

show interfaces transceiver — displays the physical status and operational status of an installed transceiver. The output also displays the transceiver's serial number.

show interfaces transceiver

Display the physical status and operational status of an installed transceiver. The output also displays the transceiver's serial number.

Syntax

```
show interfaces [tengigabitethernet slot/port | fortyGigE slot/port] transceiver
```

Parameters

tengigabitethernet	For a 10G interface, enter the keyword `tengigabitethernet` then the slot/port information.
fortyGigE	For a 40G interface, enter the keyword `fortyGigE` then the slot/port information.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show interfaces transceiver` command shown in the following example.

Line	Description
Rx Power measurement type	Output depends on the vendor, typically either "Average" or "OMA" (Receiver optical modulation amplitude).
Temp High Alarm threshold	Factory-defined setting, typically in Centigrade. Value differs between SFPs and SFP+.
Voltage High Alarm threshold	Displays the interface index number used by SNMP to identify the interface.

Line	Description
Bias High Alarm threshold	Factory-defined setting. Value can differ between SFP and SFP+.
TX Power High Alarm threshold	Factory-defined setting. Value can differ between SFP and SFP+.
RX Power High Alarm threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Temp Low Alarm threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Voltage Low Alarm threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Bias Low Alarm threshold	Factory-defined setting. Value can differ between SFP and SFP+.
TX Power Low Alarm threshold	Factory-defined setting. Value can differ between SFP and SFP+.
RX Power Low Alarm threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Temp High Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Voltage High Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Bias High Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.
TX Power High Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.
RX Power High Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Temp Low Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Voltage Low Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Bias Low Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.
TX Power Low Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Power Low Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Temperature	Current temperature of the SFPs. If this temperature crosses Temp High alarm/warning thresholds, the temperature high alarm/warning flag is set to true.

Line	Description
Voltage	Current voltage of the SFPs. If this voltage crosses voltage high alarm/warning thresholds, the voltage high alarm/ warning flag is set to true.
Tx Bias Current	Present transmission (Tx) bias current of the SFP. If this crosses bias high alarm/warning thresholds, the TX bias high alarm/warning flag is set to true. If it falls below the low alarm/warning thresholds, the TX bias low alarm/warning flag is set to true.
Tx Power	Present Tx power of the SFP. If this crosses Tx power alarm/ warning thresholds, the Tx power high alarm/warning flag is set to true. If it falls below the low alarm/warning thresholds, the Tx power low alarm/ warning flag is set to true.
Rx Power	Present receiving (Rx) power of the SFP. This value is either average Rx power or OMA. This depends on the Rx Power measurement type displayed above. If this crosses Rx power alarm/warning thresholds, the Rx power high alarm/warning flag is set to true. If it falls below the low alarm/warning thresholds, the Rx power low alarm/warning flag is set to true.
Data Ready state Bar	This field indicates that the transceiver has achieved power up and data is ready. This is set to true if data is ready to be sent and set to false if data is being transmitted.
Rx LOS state	This is the digital state of the Rx_LOS output pin. This is set to true if the operating status is down.
Tx Fault state	This is the digital state of the Tx Fault output pin.
Rate Select state	This is the digital state of the SFP rate_select input pin.
RS state	This is the reserved digital state of the pin AS(1) per SFF-8079 and RS(1) per SFF-8431.
Tx Disable state	If the admin status of the port is down then this flag is set to true.
Temperature High Alarm Flag	This can be either true or false, depending on the Current voltage value displayed above.
Voltage High Alarm Flag	This can be either true or false, depending on the Current Temperature value displayed above.
Tx Bias High Alarm Flag	This can be either true or false, depending on the present Tx bias current value displayed above.
Tx Power High Alarm Flag	This can be either true or false, depending on the Current Tx bias power value displayed above.
Rx Power High Alarm Flag	This can be either true or false, depending on the Current Rx power value displayed above.

Line	Description
Temperature Low Alarm Flag	This can be either true or false, depending on the Current Temperature value displayed above.
Voltage Low Alarm Flag	This can be either true or false, depending on the Current voltage value displayed above.
Tx Bias Low Alarm Flag	This can be either true or false, depending on the Tx bias current value displayed above.
Tx Power Low Alarm Flag	This can be either true or false, depending on the Current Tx power value displayed above.
Rx Power Low Alarm Flag	This can be either true or false, depending on the Current Rx power value displayed above.
Temperature High Warning Flag	This can be either true or false, depending on the Current Temperature value displayed above.
Voltage High Warning Flag	This can be either true or false, depending on the Current Voltage value displayed above.
Tx Bias High Warning Flag	This can be either true or false, depending on the Tx bias current value displayed above.
Tx Power High Warning Flag	This can be either true or false, depending on the Current Tx power value displayed above.
Rx Power High Warning Flag	This can be either true or false, depending on the Current Tx power value displayed above.
Temperature Low Warning Flag	This can be either true or false, depending on the Current Temperature value displayed above.
Voltage Low Warning Flag	This can be either true or false, depending on the Current Voltage value displayed above.
Tx Bias Low Warning Flag	This can be either true or false, depending on the present Tx bias current value displayed above.
Tx Power Low Warning Flag	This can be either true or false, depending on the Current Tx power value displayed above.
Rx Power Low Warning Flag	This can be either true or false, depending on the Current Rx power value displayed above.

Example

```
Dell#show interfaces gigabitethernet 1/0 transceiver
SFP is present.

SFP 0 Serial Base ID fields
SFP 0 Id                  = 0x03
SFP 0 Ext Id              = 0x04
SFP 0 Connector           = 0x07
SFP 0 Transciever Code = 0x00 0x00 0x00 0x01 0x20 0x40 0x0c
0x05
SFP 0 Encoding            = 0x01
SFP 0 BR Nominal          = 0x15
SFP 0 Length(9um) Km      = 0x00
SFP 0 Length(9um) 100m    = 0x00
SFP 0 Length(50um) 10m    = 0x1e
SFP 0 Length(62.5um) 10m  = 0x0f
SFP 0 Length(Copper) 10m  = 0x00
SFP 0 Vendor Rev          = A
SFP 0 Laser Wavelength    = 850 nm
SFP 0 CheckCodeBase       = 0x66
SFP 0 Serial Extended ID fields
SFP 0 Options             = 0x00 0x12
SFP 0 BR max= 0
SFP 0 BR min= 0
SFP 0 Vendor SN= P5N1ACE
SFP 0 Datecode            = 040528
SFP 0 CheckCodeExt        = 0x5b

SFP 1 Diagnostic Information
===================================
SFP 1 Rx Power measurement type     = Average
===================================
SFP 1 Temp High Alarm threshold       = 95.000C
SFP 1 Voltage High Alarm threshold    = 3.900V
SFP 1 Bias High Alarm threshold       = 17.000mA
SFP 1 TX Power High Alarm threshold   = 0.631mW
SFP 1 RX Power High Alarm threshold   = 1.259mW
SFP 1 Temp Low Alarm threshold        = -25.000C
SFP 1 Voltage Low Alarm threshold     = 2.700V
SFP 1 Bias Low Alarm threshold        = 1.000mA
SFP 1 TX Power Low Alarm threshold    = 0.067mW
SFP 1 RX Power Low Alarm threshold    = 0.010mW
===================================
SFP 1 Temp High Warning threshold     = 90.000C
SFP 1 Voltage High Warning threshold  = 3.700V
SFP 1 Bias High Warning threshold     = 14.000mA
SFP 1 TX Power High Warning threshold = 0.631mW
SFP 1 RX Power High Warning threshold = 0.794mW
SFP 1 Temp Low Warning threshold      = -20.000C
SFP 1 Voltage Low Warning threshold   = 2.900V
SFP 1 Bias Low Warning threshold      = 2.000mA
SFP 1 TX Power Low Warning threshold  = 0.079mW
SFP 1 RX Power Low Warning threshold  = 0.016mW
===================================
SFP 1 Temperature                     = 39.930C
SFP 1 Voltage                         = 3.293V
SFP 1 Tx Bias Current                 = 6.894mA
SFP 1 Tx Power                        = 0.328mW
SFP 1 Rx Power                        = 0.000mW
===================================
SFP 1 Data Ready state Bar            = False
SFP 1 Rx LOS state                    = True
SFP 1 Tx Fault state                  = False
SFP 1 Rate Select state               = False
SFP 1 RS state                        = False
SFP 1 Tx Disable state                = False
===================================
SFP 1 Temperature High Alarm Flag     = False
SFP 1 Voltage High Alarm Flag         = False
SFP 1 Tx Bias High Alarm Flag         = False
SFP 1 Tx Power High Alarm Flag        = False
SFP 1 Rx Power High Alarm Flag        = False
SFP 1 Temperature Low Alarm Flag      = False
SFP 1 Voltage Low Alarm Flag          = False
SFP 1 Tx Bias Low Alarm Flag          = False
SFP 1 Tx Power Low Alarm Flag         = False
SFP 1 Rx Power Low Alarm Flag         = True
```

```
==================================
!-------output truncated ------------------------!
```

Related Commands

[interface](#) — configures a physical interface on the switch.

[show ip interface](#) — displays Layer 3 information about the interfaces.

[show interfaces](#) — displays information on a specific physical interface or virtual interface.

[show inventory](#) — displays the switch type, components (including media), the Dell Networking OS version including hardware identification numbers, and configured protocols.

show range

Display all interfaces configured using the `interface range` command.

Syntax

`show range`

Command Modes

INTERFACE RANGE (config-if-range)

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell(conf-if-range-te-0/16)#show range
interface tengigabitethernet 0/16
Dell(conf-if-range-te-0/16)#
```

Related Commands

[interface](#) — configures a physical interface on the switch.

[show ip interface](#) — displays Layer 3 information about the interfaces.

[show interfaces](#) — displays information on a specific physical interface or virtual interface.

shutdown

Disable an interface.

Syntax

`shutdown`

To activate an interface, use the `no shutdown` command.

Defaults

The interface is disabled.

Command Modes	INTERFACE
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	The `shutdown` command marks a physical interface as unavailable for traffic. To discover if an interface is disabled, use the `show ip interface brief` command. Disabled interfaces are listed as down. Disabling a VLAN or a port channel causes different behavior. When you disable a VLAN, the Layer 3 functions within that VLAN are disabled. Layer 2 traffic continues to flow. Entering the `shutdown` command on a port channel disables all traffic on the port channel and the individual interfaces within the port channel. To enable a port channel, enter `no shutdown` on the port channel interface and at least one interface within that port channel. The `shutdown` and `description` commands are the only commands that you can configure on an interface that is a member of a port channel.
Related Commands	interface port-channel — creates a port channel interface. interface vlan — creates a VLAN. show ip interface — displays the interface routing status. Add the keyword `brief` to display a table of interfaces and their status.

speed (for 1000/10000/auto interfaces)

Set the speed for 1000/10000 Base-T Ethernet interfaces. Set both sides of a link to the same speed (1000/10000) or to auto or the link may not come up.

Syntax

```
speed {1000 | 10000 | auto}
```

To return to the default setting, use the `no speed {1000 | 10000 | auto}` command.

Parameters

1000	Enter the keyword `1000` to set the interface’s speed to 1000 Mb/s.
10000	Enter the keyword `10000` to set the interface’s speed to 10000 Mb/s. Auto-negotiation is enabled. For more information, refer to `negotiation auto`.
auto	Enter the keyword `auto` to set the interface to auto-negotiate its speed. Auto-negotiation is enabled. For more information, refer to `negotiation auto`.

Defaults **auto**

Command Modes INTERFACE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

This command is found on the 1000/10000 Base-T Ethernet interfaces.

When you enable `auto`, the system performs an automatic discovery to determine the optics installed and configure the appropriate speed.

When you configure a speed for the 1000/10000 interface, confirm the negotiation auto command setting. Both sides of the link must have auto-negotiation either enabled or disabled. For speed settings of 1000 or auto, the software sets the link to auto-negotiation and you cannot change that setting.

Related Commands

duplex (1000/10000 Interfaces) — configures duplex mode on physical interfaces with the speed set to 10/100.

negotiation auto — enables or disables auto-negotiation on an interface.

stack-unit portmode

Split a single 40G port into 4-10G ports on the MXL switch.

Syntax `stack-unit stack-unit port number portmode quad`

Parameters

stack-unit	Enter the stack member unit identifier of the stack member to reset. The range is 0 to 5. NOTE: The MXL switch commands accept Unit ID numbers from 0 to 5, though the MXL switch supports stacking up to three units only with the Dell Networking OS version 8.3.7.1.
number	Enter the port number of the 40G port to be split. Enter one of the following port numbers for the MXL switch: 48, 52, 56, or 60.

Defaults Disabled.

Command Modes CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Splitting a 40G port into 4x10G port is supported on standalone and stacked units.

- You cannot use split ports as stack-link to stack an MXL Switch.
- The split ports MXL switch unit cannot be a part of any stacked system.
- The unit number with the split ports must be the default (stack-unit 0).
- This set up can be verified using `show system brief` command. If the unit ID is different than 0, it must be renumbered to 0 before ports are split by using the `stackunit id renumber 0` command in EXEC mode.

The quad port must be in a default configuration before it can be split into 4x10G ports. The 40G port is lost in the config when the port is split, so be sure that the port is also removed from other L2/L3 feature configurations.

The system must be reloaded after issuing the CLI for the change to take effect.

Port Channel Commands

A link aggregation group (LAG) is a group of links that appear to a MAC client as if they were a single link according to IEEE 802.3ad. In the Dell Networking OS, a LAG is referred to as a Port Channel.

- For the MXL switch, the maximum port channel ID is 128 and the maximum members per port channel is 16.

Because each port can be assigned to only one Port Channel, and each Port Channel must have at least one port, some of those nominally available Port Channels might have no function because they could have no members if there are not enough ports installed. In the MXL 10/40GbE Switch IO Module, those ports could be provided by stack members.

NOTE: The Dell Networking OS implementation of LAG or Port Channel requires that you configure a LAG on both switches manually. For information about Dell Networking OS link aggregation control protocol (LACP) for dynamic LAGs, refer to the *Link Aggregation Control Protocol (LACP)* chapter. For more information about configuring and using Port Channels, refer to the *Dell Networking OS Configuration Guide*.

channel-member

Add an interface to the Port Channel, while in INTERFACE PORTCHANNEL mode.

Syntax

`channel-member interface`

To delete an interface from a Port Channel, use the `no channel-member interface` command.

Parameters

interface	(OPTIONAL) Enter any of the following keywords and slot/port or number information:

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

Defaults

Not configured.

Command Modes

INTERFACE PORTCHANNEL

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Use the `interface port-channel` command to access this command.

You cannot add an interface to a Port Channel if the interface contains an IP address in its configuration.

Link MTU and IP MTU considerations for Port Channels are:

- All members must have the same link MTU value and the same IP MTU value.
- The Port Channel link MTU and IP MTU must be less than or equal to the link MTU and IP MTU values configured on the channel members. For example, if the members have a link MTU of 2100 and an IP MTU 2000, the Port Channel’s MTU values cannot be higher than 2100 for link MTU or 2000 bytes for IP MTU.

When an interface is removed from a Port Channel with the `no channel-member` command, the interface reverts to its configuration prior to joining the Port Channel.

An interface can belong to only one Port Channel.

You can add up to 16 interfaces to a Port Channel on the MXL switch. The interfaces can be located on different line cards but must be the same physical type and speed (for example, all 10-Gigabit Ethernet interfaces). However, you can combine 100/1000 interfaces and GE interfaces in the same Port Channel.

If the Port Channel contains a mix of interfaces with 100 Mb/s speed and 1000 Mb/s speed, the software disables those interfaces whose speed does not match the speed of the first interface configured and enabled in the Port Channel. If that first interface goes down, the Port Channel does not change its designated speed; disable and re-enable the Port Channel or change the order of the channel members configuration to change the designated speed. If the Port Channel contains a mix of interfaces with 100 Mb/s speed and 1000 Mb/s speed, the software disables those interfaces whose speed does not match the speed of the first interface configured and enabled in the Port Channel. If that first interface goes down, the Port Channel does not change its designated speed; disable and re-enable the Port Channel or change the order of the channel members configuration to change the designated speed. For more information about Port Channels, refer to the *Dell Networking OS Configuration Guide*.

Related Commands	description — assigns a descriptive text string to the interface. interface port-channel — creates a Port Channel interface. shutdown — disables/enables the port channel.

group

Group two LAGs in a supergroup (“fate-sharing group” or “failover group”).

Syntax

`group group_number port-channel number port-channel number`

To remove an existing LAG supergroup, use the `no group group_number` command.

Parameters

group_number	Enter an integer from 1 to 32 that uniquely identifies this LAG fate-sharing group.
port-channel *number*	Enter the keywords `port-channel` then an existing LAG number. Enter this keyword/variable combination twice, identifying the two paired LAGs.

Defaults

none

Command Modes

PORT-CHANNEL FAILOVER-GROUP (conf-po-failover-grp)

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	

Examle

```
Dell(conf)#port-channel failover-group
Dell(conf-po-failover-grp)#group 1 port-channel 1 port-channel
2
Dell(conf-po-failover-grp)#
```

Related Commands

port-channel failover-group — accesses PORT-CHANNEL FAILOVER-GROUP mode to configure a LAG failover group.

show interfaces port-channel — displays information on configured Port Channel groups.

interface port-channel

Create a Port Channel interface, which is a link aggregation group (LAG) containing 16 physical interfaces on the XML switch.

Syntax

`interface port-channel` *`channel-number`*

To delete a Port Channel, use the `no interface port-channel` *`channel-number`* command.

Parameters

channel-number	For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Port Channel interfaces are logical interfaces and can be either in Layer 2 mode (by using the `switchport` command) or Layer 3 mode (by configuring an IP address). You can add a Port Channel in Layer 2 mode to a VLAN.

A Port Channel can contain both 100/1000 interfaces and GE interfaces. Based on the first interface configured in the Port Channel and enabled, the Dell Networking OS determines if the Port Channel uses 100 Mb/s or 1000 Mb/s as the common speed. For more information, refer to channel-member.

If the line card is in a Jumbo mode chassis, you can also configure the `mtu` and `ip mtu` commands. The Link MTU and IP MTU values configured on the channel members must be greater than the Link MTU and IP MTU values configured on the Port Channel interface.

NOTE: In a Jumbo-enabled system, you must configure all members of a Port Channel with the same link MTU values and the same IP MTU values.

Example

```
Dell(conf)#int port-channel 2
Dell(conf-if-po-2)#
```

Related Commands

channel-member — adds a physical interface to the LAG.

interface — configures a physical interface.

interface vlan — configures a VLAN.

shutdown — disables/enables the port channel.

minimum-links

Configure the minimum number of links in a LAG (Port Channel) that must be in “oper up” status for the LAG to be also in “oper up” status.

Syntax	`minimum-links number`
Parameters	*number* — Enter the number of links in a LAG that must be in “oper up” status. The range is from 1 to 16. The default is **1**.
Defaults	**1**
Command Modes	INTERFACE
Command History	Version 9.2(0.0) — Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only. Version 8.3.16.1 — Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	If you use this command to configure the minimum number of links in a LAG that must be in “oper up” status, the LAG must have at least that number of “oper up” links before it can be declared as up. For example, if the required minimum is four, and only three are up, the LAG is considered down.

port-channel failover-group

To configure a LAG failover group, access PORT-CHANNEL FAILOVER-GROUP mode.

Syntax	`port-channel failover-group` To remove all LAG failover groups, use the `no port-channel failover-group` command.
Defaults	none
Command Modes	CONFIGURATION
Command History	Version 9.2(0.0) — Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only. Version 8.3.16.1 — Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	This feature groups two LAGs to work in tandem as a supergroup. For example, if one LAG goes down, the other LAG is taken down automatically, providing an alternate path to reroute traffic, avoiding oversubscription on the other LAG. You can use both static and dynamic (LACP) LAGs to configure failover groups. For

more information, refer to the *Port Channel* chapter in the *Dell Networking OS Configuration Guide*.

Related Command

group — groups two LAGs in a supergroup ("fate-sharing group").

show interfaces port-channel — displays information on configured Port Channel groups.

show config

Display the current configuration of the selected LAG.

Syntax `show config`

Command Modes INTERFACE PORTCHANNEL

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell(conf-if-po-1)#show config
!
interface Port-channel 1
  no ip address
  shutdown
Dell(conf-if-po-1)#
```

show interfaces port-channel

Display information on configured Port Channel groups.

Syntax `show interfaces port-channel [channel-number] [brief]`

Parameters

channel-number	For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
brief	(OPTIONAL) Enter the keyword `brief` to display only the port channel number, the state of the port channel, and the number of interfaces in the port channel.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the S4820T.

Usage Information

The following describes the `show interfaces port-channel` command shown in the following example.

Field	Description
Port-Channel 1...	Displays the LAG's status. In the Example, the status of the LAG's LAG fate-sharing group ("Failover-group") is listed.
Hardware is...	Displays the interface's hardware information and its assigned MAC address.
Port-channel is part...	Indicates whether the LAG is part of a LAG fate-sharing group ("Failover-group").
Internet address...	States whether an IP address is assigned to the interface. If an IP address is assigned, that address is displayed.
MTU 1554...	Displays link and IP MTU.
LineSpeed	Displays the interface's line speed. For a port channel interface, it is the line speed of the interfaces in the port channel.
Members in this...	Displays the interfaces belonging to this port channel.
ARP type:...	Displays the ARP type and the ARP timeout value for the interface.
Last clearing...	Displays the time when the `show interfaces` counters were cleared.
Queueing strategy.	States the packet queuing strategy. FIFO means first in first out.
packets input...	Displays the number of packets and bytes into the interface.
Input 0 IP packets...	Displays the number of packets with IP headers, VLAN tagged headers, and MPLS headers. The number of packets may not add correctly because a VLAN tagged IP packet counts as both a VLAN packet and an IP packet.
0 64-byte...	Displays the size of packets and the number of those packets entering that interface. This information is displayed over two lines.
Received 0...	Displays the type and number of errors or other specific packets received. This information is displayed over three lines.
Output 0...	Displays the type and number of packets sent out the interface. This information is displayed over three lines.
Rate information...	Displays the traffic rate information into and out of the interface. Traffic rate is displayed in bits and packets per second.
Time since...	Displays the time since the last change in the configuration of this interface.

Example (EtherScale)

```
Dell#show interfaces port-channel
Port-channel 1 is down, line protocol is down
Hardware address is 00:1e:c9:f1:00:05, Current address is
00:1e:c9:f1:00:05
Interface index is 1107755009
Minimum number of links to bring Port-channel up is 1
Internet address is not set
Mode of IP Address Assignment : NONE
DHCP Client-ID :lag1001ec9f10005
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed auto
Members in this channel:
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 03:28:00
Queueing strategy: fifo
Input Statistics:
     0 packets, 0 bytes
     0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
     0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-
byte pkts
     0 Multicasts, 0 Broadcasts
     0 runts, 0 giants, 0 throttles
     0 CRC, 0 overrun, 0 discarded
Output Statistics:
     0 packets, 0 bytes, 0 underruns
     0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
     0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-
byte pkts
     0 Multicasts, 0 Broadcasts, 0 Unicasts
     0 throttles, 0 discarded, 0 collisions
```

User Information

The following describes the `show interfaces port-channel brief` command shown in the following example.

Field	Description
LAG	Lists the port channel number.
Mode	Lists the mode: • L3 — for Layer 3 • L2 — for Layer 2
Status	Displays the status of the port channel. • down — if the port channel is disabled (`shutdown`) • up — if the port channel is enabled (`no shutdown`)
Uptime	Displays the age of the port channel in hours:minutes:seconds.
Ports	Lists the interfaces assigned to this port channel.
(untitled)	Displays the status of the physical interfaces (up or down). • In Layer 2 port channels, an * (asterisk) indicates which interface is the primary port of the port channel. The primary port sends out interface PDU.

Field	Description
	- In Layer 3 port channels, the primary port is not indicated.

Example (brief)

```
Dell#show int po 1 brief
Codes: L - LACP Port-channel

  LAG Mode Status Uptime   Ports
  1   L3   down   00:00:00 Te 0/16 (Down)
Dell#
```

Related Commands

show lacp — displays the LACP matrix.

Time Domain Reflectometer (TDR)

TDR is useful for troubleshooting an interface that is not establishing a link; either it is flapping or not coming up at all. TDR detects open or short conditions of copper cables on 100/1000 Base-T modules.

Important Points to Remember

- The interface and port must be enabled (configured — refer to the `interface` command) before running TDR. An error message is generated if you have not enabled the interface.
- The interface on the far-end device must be shut down before running TDR.
- Because TDR is an intrusive test on an interface that is not establishing a link, do not run TDR on an interface that is passing traffic.
- When testing between two devices, do not run the test on both ends of the cable.

tdr-cable-test

Test the condition of copper cables on 100/1000 Base-T modules.

Syntax

```
tdr-cable-test interface
```

Parameters

interface	Enter the keyword `TenGigabitEthernet` then the slot/port information for the 100/1000 Ethernet interface.

Defaults none

Command Modes EXEC

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information	The interface must be enabled to run the test or an error message is generated:

```
Dell#tdr-cable-test gigabitethernet 5/2

%Error: Interface is disabled GI 5/2
```

Related Commands	show tdr — displays the results of the TDR test.

show tdr

Display the TDR test results.

Syntax	`show tdr` *`interface`*

Parameters

interface	Enter the keyword `TenGigabitEthernet` then the slot/port information for the 100/1000 Ethernet interface.

Defaults	none
Command Modes	EXEC

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

If the TDR test has not been run, an error message is generated:

```
%Error: Please run the TDR test first
```

The following describes the TDR test status.

Status	Definition
OK Status: Terminated	TDR test is complete, no fault is detected on the cable, and the test is terminated.
Length: 92 (+/- 1) meters, Status: Shorted	A short is detected on the cable. The location, in this Example is 92 meters. The short is accurate to plus or minus one meter.
Length: 93 (+/- 1) meters, Status: Open	An opening is detected on the cable. The location, in this Example is 93 meters. The open is accurate to plus or minus one meter.
Status: Impedance Mismatch	There is an impedance mismatch in the cables.

Example

```
Dell#show tdr tengigabitethernet 10/47
Time since last test: 00:00:02
  Pair A, Length: OK Status: Terminated
Pair B, Length: 92 (+/- 1) meters, Status: Short
Pair C, Length: 93 (+/- 1) meters, Status: Open
Pair D, Length: 0 (+/- 1) meters, Status: Impedance Mismatch
```

Related Commands	tdr-cable-test — runs the TDR test.

UDP Broadcast

The user datagram protocol (UDP) broadcast feature is a software-based method to forward low throughput (not to exceed 200 pps) IP/UDP broadcast traffic arriving on a physical or VLAN interface.

Important Points to Remember

- Routing information protocol (RIP) is not supported with the UDP Broadcast feature.
- If you configure this feature on an interface using the `ip udp-helper udp-port` command, the `ip directed-broadcast` command becomes ineffective on that interface.
- The existing `show interface` command has been modified to display the configured broadcast address.

debug ip udp-helper

Enable UDP debug and display the debug information on a console.

Syntax

`debug ip udp-helper`

To disable debug information, use the `no debug ip udp-helper` command.

Defaults

Debug disabled.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#debug ip udp-helper
UDP helper debugging is on

01:20:22: Pkt rcvd on Gi 5/0 with IP DA (0xffffffff) will be
sent on Gi 5/1 Gi 5/2
Vlan 3

01:44:54: Pkt rcvd on Gi 7/0 is handed over for DHCP
processing.
```

Related Commands

ip udp-broadcast-address — configures a UDP IP address for broadcast.

ip udp-helper udp-port — enables the UDP broadcast feature on an interface.

show ip udp-helper — displays the configured UDP helper(s) on all interfaces.

ip udp-broadcast-address

Configure an IP UDP address for broadcast.

Syntax	`ip udp-broadcast-address address` To delete the configuration, use the `no ip udp-broadcast-address address` command.
Parameters	*address* — Enter an IP broadcast address in dotted decimal format (A.B.C.D).
Defaults	Not configured.
Command Modes	INTERFACE (config-if)
Command History	**Version 8.3.16.1** — Enter an IP broadcast address in dotted decimal format (A.B.C.D).
Usage Information	When a UDP broadcast packet is flooded out of an interface, and the outgoing interface is configured using this command, the outgoing packet's IP destination address is replaced with the configured broadcast address.
Related Commands	debug ip udp-helper — enables debug and displays the debug information on a console. show ip udp-helper — displays the configured UDP helpers on all interfaces.

ip udp-helper udp-port

Enable the UDP broadcast feature on an interface either for all UDP ports or a specified list of UDP ports.

Syntax	`ip udp-helper udp-port [udp-port-list]` To disable the UDP broadcast on a port, use the `no ip udp-helper udp-port [udp-port-list]` command.
Parameters	*udp-port-list* — (OPTIONAL) Enter up to 16 comma-separated UDP port numbers. NOTE: If you do not use this option, all UDP ports are considered by default.

Defaults	none
Command Modes	INTERFACE (config-if)

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

If you configure the `ip helper-address` command and `ip udp-helper udp-port` command, the behavior is that the UDP broadcast traffic with port numbers 67/68 is unicast relayed to the DHCP server per the `ip helper-address` configuration. This occurs regardless if the `ip udp-helper udp-port` command contains port numbers 67/68 or not.

If you only configure the `ip udp-helper udp-port` command, all the UDP broadcast traffic is flooded, including ports 67/68 traffic if those ports are part of the `udp-port-list`.

Related Commands

ip helper-address — configures the destination broadcast or host address for the DHCP server.

debug ip udp-helper — enables debug and displays the debug information on a console.

show ip udp-helper — displays the configured UDP helpers on all interfaces.

show ip udp-helper

Display the configured UDP helpers on all interfaces.

Syntax	`show ip udp-helper`
Defaults	none
Command Modes	EXEC

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show ip udp-helper
--------------------------------------------------
Port     UDP  port  list
--------------------------------------------------
Gi 10/0  656, 658
Gi 10/1  All
```

Related Commands

debug ip udp-helper — enables debug and displays the debug information on a console.

ip udp-broadcast-address — configures a UDP IP address for broadcast.

ip udp-helper udp-port — enables the UDP broadcast feature on an interface either for all UDP ports or a specified list of UDP ports.

Enhanced Validation of Interface Ranges

This functionality is supported on the MXL platform.

You can avoid specifying spaces between the range of interfaces, separated by commas, that you configure by using the `interface range` command. For example, if you enter a list of interface ranges, such as `interface range fo 2/0-1,te 10/0,gi 3/0,fa 0/0`, this configuration is considered valid. The comma-separated list is not required to be separated by spaces in between the ranges. You can associate multicast MAC or hardware addresses to an interface range and VLANs by using the `mac-address-table static` *`multicast-mac-address`* `vlan` *`vlan-id`* `output-range` *`interface`* command.

22

IPv4 Routing

The basic IPv4 commands are supported by Dell Networking Operating System (OS).

arp

To associate an IP address with a multicast MAC address in the switch when you configure multicast mode of the network load balancing (NLB), use the address resolution protocol (ARP).

Syntax

`arp ip-address multicast-mac-address interface`

To remove an ARP address, use the `no arp ip-address` command.

Parameters

ip-address	Enter an IP address in dotted decimal format.
multicast-mac-address	Enter a 48–bit hexadecimal address in MAC address in nn:nn:nn:nn:nn:nn format for the static MAC address to be used to switch multicast traffic..
interface	(OPTIONAL) Enter any of the following keywords and slot/port or number information: • For the Management interface, enter the keyword `ManagementEthernet` then the slot/port information. The slot range is from 0 to 1 and the port range is 0. • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • The interface specified here must be one of the interfaces configured using the `{output-range | output} interface` option with the `mac-address-table static` command.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

Version 9.3(0.0)	Added the support for association of an IP address with multicast MAC address on the MXL platform.

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

For multicast mode of NLB, to associate an IP address with a multicast MAC address in the switch, use address resolution protocol (ARP) by entering the `arp` *`ip-address multicast-mac-address`* command in Global configuration mode. This setting causes the multicast MAC address to be mapped to the cluster IP address for NLB mode of operation of the switch.

You cannot use Class D or Class E IP addresses or zero IP address (0.0.0.0) when creating a static ARP. Zero MAC addresses (00:00:00:00:00:00) are also invalid.

Related Commands

clear arp-cache — clears dynamic ARP entries from the ARP table.

show arp — displays the ARP table.

arp learn-enable

Enable ARP learning using gratuitous ARP.

Syntax `arp learn-enable`

Defaults Disabled

Command Modes CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

arp retries

Set the number of ARP retries in case the system does not receive an ARP reply in response to an ARP request.

Syntax `arp retries` *`number`*

Parameters

number	Enter the number of retries. The range is from 5 to 20. The default is **5**.

Defaults **5**

Command Modes CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information	Retries are 20 seconds apart.
Related Commands	show arp retries — displays the configured number of ARP retries.

arp timeout

Set the time interval for an ARP entry to remain in the ARP cache.

Syntax

```
arp timeout minutes
```

Parameters

minutes	Enter the number of minutes. The range is from 0 to 35790. The default is **240 minutes**.

Defaults	**240 minutes** (4 hours)
Command Modes	INTERFACE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands	show interfaces — displays the ARP timeout value for all available interfaces.

clear arp-cache

Clear the dynamic ARP entries from a specific interface or optionally delete (`no-refresh`) ARP entries from the content addressable memory (CAM).

Syntax

```
clear arp-cache [interface | ip ip-address] [no-refresh]
```

Parameters

interface — (OPTIONAL) Enter the following keywords and slot/port or number information:

- For the Management interface, enter the keyword `ManagementEthernet` then the slot/port information. The slot range is from 0 to 1 and the port range is 0.
- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

ip *ip-address*	(OPTIONAL) Enter the keyword `ip` then the IP address of the ARP entry you wish to clear.
no-refresh	(OPTIONAL) Enter the keywords `no-refresh` to delete the ARP entry from CAM. Or use this option with `interface` or `ip ip-address` to specify which dynamic ARP entries you want to delete. **NOTE:** Transit traffic may not be forwarded during the period when deleted ARP entries are resolved again and re-installed in CAM. Use this option with extreme caution.

Command Modes EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

clear host

Remove one or all dynamically learned host table entries.

Syntax `clear host name`

Parameters

name	Enter the name of the host to delete. Enter `*` to delete all host table entries.

Command Modes EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

clear ip fib stack-unit

Clear all forwarding information base (FIB) entries in the specified stack unit (use this command with caution, refer to *Usage Information*.)

Syntax `clear ip fib stack-unit unit-number`

Parameters

unit-number	Enter the number of the stack unit. The range is from 0 to 5.

Command Modes

EXEC

EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To clear Layer 3 CAM inconsistencies, use this command.

⚠ **CAUTION: Executing this command causes traffic disruption.**

Related Commands

show ip fib stack-unit — shows FIB entries.

clear ip route

Clear one or all routes in the routing table.

Syntax

```
clear ip route {* | ip-address mask}
```

Parameters

*	Enter an asterisk (*) to clear all learned IP routes.
ip-address mask	Enter a specific IP address and mask in dotted decimal format to clear that IP address from the routing table.

Command Modes

EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

ip route — assigns an IP route to the switch.

show ip route — views the routing table.

show ip route summary — views a summary of the routing table.

clear tcp statistics

Clear TCP counters.

Syntax

```
clear tcp statistics
```

Command Modes

EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

debug arp

View information on ARP transactions.

Syntax `debug arp [interface] [count value]`

To stop debugging ARP transactions, use the `no debug arp` command.

Parameters

interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For the Management interface, enter the keyword `ManagementEthernet` then the slot/port information. The slot range is from 0 to 1 and the port range is 0. • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.
count *value*	(OPTIONAL) Enter the keyword `count` then the count value. The range is from 1 to 65534.

Defaults none

Command Modes EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information To stop packets from flooding the user terminal when debugging is turned on, use the `count` option.

debug ip dhcp

Enable debug information for dynamic host configuration protocol (DHCP) relay transactions and display the information on the console.

Syntax `debug ip dhcp`

To disable debug, use the `no debug ip dhcp` command.

Defaults Debug disabled

Command Modes EXEC Privilege

Command History	**Version 8.3.16.1**	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#debug ip dhcp
00:12:21 : %RELAY-I-PACKET: BOOTP REQUEST (Unicast) received
at interface 113.3.3.17 BOOTP
Request, hops = 0, XID = 0xbf05140f, secs = 0, hwaddr =
00:60:CF:20:7B:8C, giaddr = 0.0.0.0
00:12:21 : %RELAY-I-BOOTREQUEST: Forwarded BOOTREQUEST for
00:60:CF:20:7B:8C to 14.4.4.2
00:12:26 : %RELAY-I-PACKET: BOOTP REQUEST (Unicast) received
at interface 113.3.3.17 BOOTP
Request, hops = 0, XID = 0xbf05140f, secs = 5, hwaddr =
00:60:CF:20:7B:8C, giaddr = 0.0.0.0
00:12:26 : %RELAY-I-BOOTREQUEST: Forwarded BOOTREQUEST for
00:60:CF:20:7B:8C to 14.4.4.2
00:12:40 : %RELAY-I-PACKET: BOOTP REQUEST (Unicast) received
at interface 113.3.3.17 BOOTP
Request, hops = 0, XID = 0xda4f9503, secs = 0, hwaddr =
00:60:CF:20:7B:8C, giaddr = 0.0.0.0
00:12:40 : %RELAY-I-BOOTREQUEST: Forwarded BOOTREQUEST for
00:60:CF:20:7B:8C to 14.4.4.2
00:12:42 : %RELAY-I-PACKET: BOOTP REPLY (Unicast) received at
interface 14.4.4.1 BOOTP Reply,
hops = 0, XID = 0xda4f9503, secs = 0, hwaddr = 00:60:CF:20:7B:
8C, giaddr = 113.3.3.17
00:12:42 : %RELAY-I-BOOTREPLY: Forwarded BOOTREPLY for
00:60:CF:20:7B:8C to 113.3.3.254
00:12:42 : %RELAY-I-PACKET: BOOTP REQUEST (Unicast) received
at interface 113.3.3.17 BOOTP
Request, hops = 0, XID = 0xda4f9503, secs = 0, hwaddr =
00:60:CF:20:7B:8C, giaddr = 0.0.0.0
00:12:42 : %RELAY-I-BOOTREQUEST: Forwarded BOOTREQUEST for
00:60:CF:20:7B:8C to 14.4.4.2
00:12:42 : %RELAY-I-PACKET: BOOTP REPLY (Unicast) received at
interface 14.4.4.1 BOOTP Reply,
hops = 0, XID = 0xda4f9503, secs = 0, hwaddr = 00:60:CF:20:7B:
8C, giaddr = 113.3.3.17
00:12:42 : %RELAY-I-BOOTREPLY: Forwarded BOOTREPLY for
00:60:CF:20:7B:8C to 113.3.3.254
Dell#
```

Related Commands

ip helper-address — specifies the destination broadcast or host address for the DHCP server request.

ip helper-address hop-count disable — disables the hop-count increment for the DHCP relay agent.

debug ip icmp

View information on the internal control message protocol (ICMP).

Syntax

`debug ip icmp [`*`interface`*`] [count `*`value`*`]`

To disable debugging, use the `no debug ip icmp` command.

Parameters

interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For the Management interface, enter the keyword `ManagementEthernet` then the slot/port information. The slot range is from 0 to 1 and the port range is 0. • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.
count *value*	(OPTIONAL) Enter the keyword `count` then the count value. The range is from 1 to 65534. The default is **Infinity**.

Command Modes

EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
ICMP: echo request rcvd from src 40.40.40.40
ICMP: src 40.40.40.40, dst 40.40.40.40, echo reply
ICMP: src 40.40.40.40, dst 40.40.40.40, echo reply
ICMP: echo request sent to dst 40.40.40.40
ICMP: echo request rcvd from src 40.40.40.40
ICMP: src 40.40.40.40, dst 40.40.40.40, echo reply
ICMP: src 40.40.40.40, dst 40.40.40.40, echo reply
ICMP: echo request sent to dst 40.40.40.40
```

Usage Information

To stop packets from flooding the user terminal when debugging is turned on, use the `count` option.

debug ip packet

View a log of IP packets sent and received.

Syntax

`debug ip packet [access-group name] [count value] [interface]`

To disable debugging, use the `no debug ip packet [access-group name] [count value] [interface]` command.

Parameters

access-group *name*	Enter the keywords `access-group` then the access list name (maximum 16 characters) to limit the debug output based on the defined rules in the ACL.

count *value*	(OPTIONAL) Enter the keyword `count` then the count value. The range is from 1 to 65534. The default is `Infinity`.
interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For the Management interface, enter the keyword `ManagementEthernet` then the slot/port information. The slot range is from 0 to 1 and the port range is 0. • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

Command Modes

EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `debug ip packet` command in the following example.

Field	Description
s=	Lists the source address of the packet and the name of the interface (in parentheses) that received the packet.
d=	Lists the destination address of the packet and the name of the interface (in parentheses) through which the packet is being sent out on the network.
len	Displays the packet's length.
sending, rcvd, fragment, sending broad/multicast proto, unroutable	The last part of each line lists the status of the packet.
TCP src=	Displays the source and destination ports, the sequence number, the acknowledgement number, and the window size of the packets in that TCP packets.
UDP src=	Displays the source and destination ports for the UDP packets.
ICMP type=	Displays the ICMP type and code.
IP Fragment	States that it is a fragment and displays the unique number identifying the fragment (Ident) and the offset (in 8-byte

Field	Description
	units) of this fragment (fragment offset) from the beginning of the original datagram.

Example

```
IP: s=10.1.2.62 (local), d=10.1.2.206 (Ma 0/0), len 54, sending
    TCP src=23, dst=40869, seq=2112994894, ack=606901739,
win=8191 ACK PUSH
IP: s=10.1.2.206 (Ma 0/0), d=10.1.2.62, len 40, rcvd
    TCP src=0, dst=0, seq=0, ack=0, win=0
IP: s=10.1.2.62 (local), d=10.1.2.206 (Ma 0/0), len 226,
sending
    TCP src=23, dst=40869, seq=2112994896, ack=606901739,
win=8192 ACK PUSH
IP: s=10.1.2.216 (Ma 0/0), d=10.1.2.255, len 78, rcvd
    UDP src=0, dst=0
IP: s=10.1.2.62 (local), d=10.1.2.3 (Ma 0/0), len 1500,
sending fragment
    IP Fragment, Ident = 4741, fragment offset = 0
    ICMP type=0, code=0
IP: s=10.1.2.62 (local), d=10.1.2.3 (Ma 0/0), len 1500,
sending fragment
    IP Fragment, Ident = 4741, fragment offset = 1480
IP: s=40.40.40.40 (local), d=224.0.0.5 (Gi 4/11), len 64,
sending broad/multicast
proto=89
IP: s=40.40.40.40 (local), d=224.0.0.6 (Gi 4/11), len 28,
sending broad/multicast
proto=2
IP: s=0.0.0.0, d=30.30.30.30, len 100, unroutable
   ICMP type=8, code=0
IP: s=0.0.0.0, d=30.30.30.30, len 100, unroutable
   ICMP type=8, code=0
```

Usage Information

To stop packets from flooding the user terminal when debugging is turned on, use the `count` option.

The `access-group` option supports only the equal to (`eq`) operator in TCP ACL rules. Port operators not equal to (`neq`), greater than (`gt`), less than (`lt`), or `range` are not supported in access-group option (refer to the following example). ARP packets (`arp`) and Ether-type (`ether-type`) are also not supported in the `access-group` option. The entire rule is skipped to compose the filter.

The `access-group` option pertains to:

- IP protocol number: from 0 to 255
- Internet control message protocol (`icmp`) but not the ICMP message type (from 0 to 255)
- Any internet protocol (`ip`)
- Transmission Control Protocol (`tcp`) but not on the `rst`, `syn`, or `urg` bits
- User Datagram Protocol (`udp`)

In the case of ambiguous access control list rules, the `debug ip packet access-control` command is disabled. A message appears identifying the error (refer to the Example below).

Example (Error Messages)

```
Dell#debug ip packet access-group test
%Error: port operator GT not supported in access-list debug
%Error: port operator LT not supported in access-list debug
%Error: port operator RANGE not supported in access-list debug
%Error: port operator NEQ not supported in access-list debug

Dell#00:10:45: %RPM0-P:CP
%IPMGR-3-DEBUG_IP_PACKET_ACL_AMBIGUOUS_EXP: Ambiguous rules not
supported in access-list debug, access-list debugging is
turned off
Dell#
```

ip address

Assign a primary and secondary IP address to the interface.

Syntax

`ip address` *`ip-address mask`* `[secondary]`

To delete an IP address from an interface, use the `no ip address [`*`ip-address`*`]` command.

Parameters

ip-address	Enter an IP address in dotted decimal format.
mask	Enter the mask of the IP address in slash prefix format (for example, /24).
secondary	(OPTIONAL) Enter the keyword `secondary` to designate the IP address as the secondary address.

Defaults Not configured.

Command Modes INTERFACE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information You must be in INTERFACE mode before you add an IP address to an interface. Assign an IP address to an interface prior to entering ROUTER OSPF mode.

ip directed-broadcast

Enables the interface to receive directed broadcast packets.

Syntax

`ip directed-broadcast`

To disable the interface from receiving directed broadcast packets, use the `no ip directed-broadcast` command.

Defaults

Disabled (that is, the interface does not receive directed broadcast packets)

Command Modes

INTERFACE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

ip domain-list

Configure names to complete unqualified host names.

Syntax

`ip domain-list` *`name`*

To remove the name, use the `no ip domain-list` *`name`* command.

Parameters

name	Enter a domain name to be used to complete unqualified names (that is, incomplete domain names that cannot be resolved).

Defaults

Disabled.

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To configure a list of possible domain names, configure the `ip domain-list` command up to six times.

If you configure both the `ip domain-name` and `ip domain-list` commands, the software tries to resolve the name using the `ip domain-name` command. If the name is not resolved, the software goes through the list of names configured with the `ip domain-list` command to find a match.

To enable dynamic resolution of hosts, use the following steps:

- specify a domain name server with the `ip name-server` command
- enable DNS with the `ip domain-lookup` command

To view current bindings, use the `show hosts` command. To view a DNS-related configuration, use the `show running-config resolve` command.

Related Commands

ip domain-name — specifies a DNS server.

ip domain-lookup

To address resolution (that is, DNS), enable dynamic host-name.

Syntax	`p domain-lookup` To disable DNS lookup, use the `no ip domain-lookup` command.
Defaults	Disabled.
Command Modes	CONFIGURATION
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	To fully enable DNS, also specify one or more domain name servers with the `ip name-server` command. The Dell Networking OS does not support sending DNS queries over a VLAN. DNS queries are sent out all other interfaces, including the Management port. To view current bindings, use the `show hosts` command.
Related Commands	ip name-server — specifies a DNS server. show hosts — Views the current bindings.

ip domain-name

Configure one domain name for the switch.

Syntax	`ip domain-name` *`name`* To remove the domain name, use the `no ip domain-name` command.
Parameters	*name* — Enter one domain name to be used to complete unqualified names (that is, incomplete domain names that cannot be resolved).
Defaults	Not configured.
Command Modes	CONFIGURATION
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

You can only configure one domain name with the `ip domain-name` command. To configure more than one domain name, configure the `ip domain-list` command up to six times.

To enable dynamic resolution of hosts, use the following steps:

- specify a domain name server with the `ip name-server` command
- enable DNS with the `ip domain-lookup` command

To view current bindings, use the `show hosts` command.

Related Commands

ip domain-list — configures additional names.

ip helper-address

Specify the address of a DHCP server so that DHCP broadcast messages can be forwarded when the DHCP server is not on the same subnet as the client.

Syntax

`ip helper-address` *`ip-address`*

To remove a DHCP server address, use the `no ip helper-address` command.

Parameters

ip-address	Enter an IP address in dotted decimal format (A.B.C.D).

Defaults

Not configured.

Command Modes

INTERFACE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

You can add multiple DHCP servers by entering the `ip helper-address` command multiple times. If multiple servers are defined, an incoming request is sent simultaneously to all configured servers and the reply is forwarded to the DHCP client.

The Dell Networking OS uses standard DHCP ports, that is UDP ports 67 (server) and 68 (client) for DHCP relay services. It listens on port 67 and if it receives a broadcast, the software converts it to unicast, and forwards to it to the DHCP-server with source port=68 and destination port=67.

The server replies with source port=67, destination port=67 and the system forwards to the client with source port=67, destination port=68.

ip helper-address hop-count disable

Disable the hop-count increment for the DHCP relay agent.

Syntax	`ip helper-address hop-count disable` To re-enable the hop-count increment, use the `no ip helper-address hop-count disable` command.
Defaults	Enabled; the hops field in the DHCP message header is incremented by default.
Command Modes	CONFIGURATION
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	This command disables the incrementing of the hops field when boot requests are relayed to a DHCP server through the Dell Networking OS. If the incoming boot request already has a non-zero hops field, the message is relayed with the same value for hops. However, the message is discarded if the hops field exceeds 16, to comply with the relay agent behavior specified in RFC 1542.
Related Commands	ip helper-address — specifies the destination broadcast or host address for DHCP server requests. show running-config — displays the current configuration and changes from the default values.

ip host

Assign a name and IP address to be used by the host-to-IP address mapping table.

Syntax	`ip host name ip-address` To remove an IP host, use the `no ip host name [ip-address]` command.
Parameters	
Defaults	Not configured.
Command Modes	CONFIGURATION
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

Parameters:

name	Enter a text string to associate with one IP address.
ip-address	Enter an IP address, in dotted decimal format, to be mapped to the name.

ip icmp source-interface

Enable the ICMP error and unreachable messages to be sent with the source interface IP address, such as the loopback address, instead of the hops of the preceding devices along the network path to be used for easy debugging and diagnosis of network disconnections and reachability problems with IPv4 packets. This functionality is supported on the MXL platform.

Syntax

```
ip icmp source-interface interface
```

Parameters

interface	Enter one of the following keywords and slot/port or number information:

- For a Management Ethernet interface, enter the keyword `managementethernet`.

  NOTE: When you configure the capability to enable the loopback IP address to be sent for easy debugging and diagnosis (IP addresses of the devices for which the ICMP source interface is configured), the source IP address of the outgoing ICMP error message is modified, although the packets are not sent out using the configured interface. Because the management interface is configured without any parameters such as the IP address, it is treated to the management interface of the primary unit or the existing unit.
- For a Loopback interface, enter the keyword `loopback`. The range is from 0 to 16383.
- For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet`.
- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet`.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE`.
- For a VLAN interface, enter the keyword `vlan`. The range is from 1 to 4094.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

Version 9.3(0.0)	Introduced on the MXL platform.

Usage Information

You can enable the mechanism to configure the source or the originating interface from which the packet (the device that generates the ICMP error messages) is received by the switch to send the loopback address instead of its source IP address to be used in the ICMP unreachable messages and in the `traceroute` command output. The loopback address must be unique in a particular domain.

In network environments that contain a large number of devices, ranging up to thousands of systems, and with each device configured for equal-cost multipath

(ECMP) links, you cannot effectively and optimally use the traceroute and ping applications to examine the network reachablity and identify any broken links for diagnostic purposes. In such cases, if the reply that is obtained from each hop on the network path contains the IP address of the adjacent, neighboring interface from which the packet is received, it is difficult to employ the ping and traceroute utilites. You can enable the ICMP unreachable messages to contain the loopback address of the source device instead of the previous hop's IP address to be able to easily and quickly identify the device and devices along the path because the DNS server maps the loopback IP address to the hostname and does not translate the IP address of every interface of the switch to the hostname.

Example

```
Dell(conf)#ip icmp source-interface tengigabitethernet 0/0
Dell(conf)#
```

ipv6 icmp source-interface

Enable the ICMP error and unreachable messages to be sent with the source interface IP address, such as the loopback address, instead of the hops of the preceding devices along the network path to be used for easy debugging and diagnosis of network disconnections and reachability problems with IPv6 packets. This functionality is supported on the MXL platform.

Syntax

```
ipv6 icmp source-interface interface
```

Parameters

interface	Enter one of the following keywords and slot/port or number information: • For a Management Ethernet interface, enter the keyword `managementethernet`. **NOTE:** When you configure the capability to enable the loopback IP address to be sent for easy debugging and diagnosis (IP addresses of the devices for which the ICMP source interface is configured), the source IP address of the outgoing ICMP error message is modified, although the packets are not sent out using the configured interface. Because the management interface is configurable only without any parameters such as the IP address, it is treated to the management interface of the primary unit or the existing unit. • For a Loopback interface, enter the keyword `loopback`. The range is from 0 to 16383. • For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet`. • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet`. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE`. • For a VLAN interface, enter the keyword `vlan`. The range is from 1 to 4094.

Defaults	Not configured.
Command Modes	CONFIGURATION
Command History	**Version 9.3(0.0)** Introduced on the MXL platform.

Usage Information

You can enable the mechanism to configure the source or the originating interface from which the packet (the device that generates the ICMP error messages) is received by the switch to send the loopback address instead of its source IP address to be used in the ICMP unreachable messages and in the `traceroute` command output. The loopback address must be unique in a particular domain.

In network environments that contain a large number of devices, ranging up to thousands of systems, and with each device configured for equal-cost multipath (ECMP) links, you cannot effectively and optimally use the traceroute and ping applications to examine the network reachablity and identify any broken links for diagnostic purposes. In such cases, if the reply that is obtained from each hop on the network path contains the IP address of the adjacent, neighboring interface from which the packet is received, it is difficult to employ the ping and traceroute utilites. You can enable the ICMP unreachable messages to contain the loopback address of the source device instead of the previous hop's IP address to be able to easily and quickly identify the device and devices along the path because the DNS server maps the loopback IP address to the hostname and does not translate the IP address of every interface of the switch to the hostname.

Example

```
Dell(conf)#ipv6 icmp source-interface tengigabitethernet 0/0
Dell(conf)#
```

ip max-frag-count

Set the maximum number of fragments allowed in one packet for packet re-assembly.

Syntax

`ip max-frag-count` *`count`*

To place no limit on the number of fragments allowed, use the `no ip max-frag-count` command.

Parameters

count	Enter a number for the number of fragments allowed for re-assembly. The range is from 2 to 256.

Defaults	No limit is set on number of fragments allowed.
Command Modes	CONFIGURATION
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To avoid denial of service (DOS) attacks, keep the number of fragments allowed for re-assembly low.

ip name-server

Enter up to six IPv4 addresses of name servers. The order you enter the addresses determines the order of their use.

Syntax

`ip name-server` *`ipv4-address`* `[`*`ipv4-address2...ipv4-address6`*`]`

To remove a name server, use the `no ip name-server` *`ip-address`* command.

Parameters

ipv4-address	Enter the IPv4 address, in dotted decimal format, of the name server to be used.
ipv4-address2... *ipv4-address6*	(OPTIONAL) Enter up five more IPv4 addresses, in dotted decimal format, of name servers to be used. Separate the addresses with a space.

Defaults

No name servers are configured.

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The system does not support sending DNS queries over a VLAN. DNS queries are sent out on all other interfaces, including the Management port.

ip proxy-arp

Enable proxy ARP on an interface.

Syntax

`ip proxy-arp`

To disable proxy ARP, use the `no ip proxy-arp` command.

Defaults

Enabled.

Command Modes

INTERFACE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

show ip interface — displays the interface routing status and configuration.

ip route

Assign a static route to the switch.

Syntax

```
ip route {destination mask {ip-address | interface [ip-address]
| [distance] | [permanent] | tag tag-value}}
```

To delete a specific static route, use the `no ip route destination mask` command.

To delete all routes matching a certain route, use the `no ip route destination mask` command.

Parameters

destination	Enter the IP address in dotted decimal format of the destination device.
mask	Enter the mask in the slash prefix format (/x) of the destination IP address.
ip-address	Enter the IP address of the forwarding router in dotted decimal format.
interface	Enter the keyword `interface` then the slot/port number. • For a Loopback interface, enter the keyword `loopback` then a number from zero (0) to 16383. • For the null interface, enter the keyword `null` then zero (0). • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.
distance	(OPTIONAL) Enter the value of the distance metric assigned to the route. The range is from 1 to 255.
permanent	(OPTIONAL) Enter the keyword `permanent` to specify that the route must not be removed even if the interface assigned to that route goes down. The route must be currently active to be installed in the routing table. If you disable the interface, the route is removed from the routing table.
tag *tag-value*	(OPTIONAL) Enter the keyword `tag` then a number to assign to the route. The range is from 1 to 4294967295.

Defaults	Not configured.
Command Modes	CONFIGURATION
Command History	**Version 9.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Using the following example of a static route: ip route 33.33.33.0 /24 tengigabitethernet 0/0 172.31.5.43

- The software installs a next hop that is not on the directly connected subnet but which recursively resolves to a next hop on the interface's configured subnet. In the example, if gig 0/0 has an ip address on subnet 2.2.2.0 and if 172.31.5.43 recursively resolves to 2.2.2.0, the system installs the static route.
- When the interface goes down, the system withdraws the route.
- When the interface comes up, the system re-installs the route.
- When recursive resolution is "broken," the system withdraws the route.
- When recursive resolution is satisfied, the system re-installs the route.

Related Commands

show ip route — views the switch routing table.

ip source-route

Enable the system to forward IP packets with source route information in the header.

Syntax

`ip source-route`

To drop packets with source route information, use the `no ip route-source` command.

Defaults	Enabled.
Command Modes	CONFIGURATION
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

ip tcp initial-time

Define the wait duration in seconds for the TCP connection to be established. This command is supported on the MXL platform.

Syntax

`ip tcp initial-time <8-75>`

To restore the default behavior, which causes the wait period to be set as eight seconds, use the `no ip tcp initial-time` command.

Parameters	*<8-75>*	Wait duration in seconds for the TCP connection to be established.

Command Modes CONFIGURATION

Command History	**Version 9.3(0.0)**	Introduced on the MXL platform.

Usage Information You can configure the amount of time for which the device must wait before it attempts to establish a TCP connection. Using this capability, you can limit the wait times for TCP connection requests. Upon responding to the initial SYN packet that requests a connection to the router for a specific service (such as SSH or BGP) with a SYN ACK, the router waits for a period of time for the ACK packet to be sent from the requesting host that will establish the TCP connection.

show ip tcp initial-time

Displays the interval that you configured for the device to wait before the TCP connection is attempted to be established. This command is supported on the MXL switch.

Syntax `show ip tcp initial-time`

Command Modes EXEC

EXEC Privilege

Command History	**Version 9.3(0.0)**	Introduced on the MXL 10/40GbE Switch IO Module platform.

ip unreachables

Enable the generation of internet control message protocol (ICMP) unreachable messages.

Syntax `ip unreachables`

To disable the generation of ICMP messages, use the `no ip unreachables` command.

Defaults Disabled.

Command Modes INTERFACE

Command History	**Version 8.3.16.1**	Introduced on the MXL 10/40GbE Switch IO Module.

management route

Configure a static route that points to the Management interface or a forwarding router.

Syntax	`management route {{`*`ipv4-address]/mask`*` | {`*`forwarding-router-address`*` | managementethernet}` To remove a static route, use the `no management route{{`*`ip-address mask`*` | {`*`ipv6-address prefix-length`*`}}{`*`forwarding-router-address`*` | managementethernet}` command.

Parameters

ipv4-address]/ mask	Enter an IPv4 Address (A.B.C.D) then the prefix-length for the IP address of the management interface.
forwarding-router-address	Enter an IPv4 address of a forwarding router.
managementethernet	Enter the keyword `managementethernet` for the Management interface.

Defaults	Not configured.	
Command Modes	CONFIGURATION	
Command History	**Version 8.3.16.1**	Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	When a static route (or a protocol route) overlaps with Management static route, the static route (or a protocol route) is preferred over the Management Static route. Also, Management static routes and the Management Connected prefix are not reflected in the hardware routing tables. Separate routing tables are maintained for IPv4 and IPv6 management routes. This command manages both tables.	
Related Commands	interface ManagementEthernet — configures the Management port on the system.	

show arp

Display the ARP table.

Syntax

```
show arp [interface interface | ip ip-address [mask] |
macaddress mac-address [mac-address mask]] [static | dynamic]
[summary]
```

Parameters

interface *interface*	(OPTIONAL) Enter the following keywords and slot/port or number information: • For the Management interface, enter the keyword `managementethernet` then the slot/port information. • For a Port Channel interface, enter the keyword `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.
ip *ip-address mask*	(OPTIONAL) Enter the keyword `ip` then an IP address in the dotted decimal format. Enter the optional IP address mask in the slash prefix format (/ x).
macaddress *mac-address mask*	(OPTIONAL) Enter the keyword `macaddress` then a MAC address in nn:nn:nn:nn:nn:nn format. Enter the optional MAC address mask in nn:nn:nn:nn:nn format also.
static	(OPTIONAL) Enter the keyword `static` to view entries entered manually.
dynamic	(OPTIONAL) Enter the keyword `dynamic` to view dynamic entries.
summary	(OPTIONAL) Enter the keyword `summary` to view a summary of ARP entries.

Command Modes

EXEC Privilege

Command History

Version 9.4.0.0	Added usage information for Clear arp-cache.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following example shows two VLANs that are associated with a private VLAN (PVLAN) (refer to Private VLAN (PVLAN)).

If you have entered the `'clear arp-cache'` command to remove a large number of ARP entries and the command is still being processed in the background, an error message is displayed as follows if you attempt to enter the `'show arp'` command: `"Clear arp in-progress.Please try after sometime!`

The following describes the `show arp` command shown in the following example.

Row Heading	Description
Protocol	Displays the protocol type.

Row Heading	Description
Address	Displays the IP address of the ARP entry.
Age(min)	Displays the age (in minutes) of the ARP entry.
Hardware Address	Displays the MAC address associated with the ARP entry.
Interface	Displays the first two letters of the interfaces type and the slot/port associated with the ARP entry.
VLAN	Displays the VLAN ID, if any, associated with the ARP entry.
CPU	Lists which CPU the entries are stored on.

Example

```
Dell>show arp

Protocol Address     Age(min) Hardware Address Interface VLAN
CPU
-----------------------------------------------------
Internet 10.11.8.6     167    00:01:e9:45:00:03 Ma 0/0 -
CP
Internet 10.11.68.14   124    00:01:e9:45:00:03 Ma 0/0 -
CP
Internet 10.11.209.254 0      00:01:e9:45:00:03 Ma 0/0 -
CP
```

Example (Private VLAN)

NOTE: In this example, Line 1 shows community VLAN 200 (in primary VLAN 10) in a PVLAN. Line 2 shows primary VLAN 10.

```
Dell#show arp
Protocol Address  Age(min) Hardware Address  Interface VLAN
CPU
---------------------------------------------------------------
Internet 5.5.5.1       -  00:01:e8:43:96:5e  -      Vl 10 pv
200 CP
Internet 5.5.5.10      -  00:01:e8:44:99:55  -      Vl
10       CP
Internet 10.1.2.4      1  00:01:e8:d5:9e:e2  Ma 0/0
-            CP
Internet 10.10.10.4    1  00:01:e8:d5:9e:e2  Ma 0/0
-            CP
Internet 10.16.127.53  1  00:01:e8:d5:9e:e2  Ma 0/0
-            CP
Internet 10.16.134.254 20 00:01:e8:d5:9e:e2  Ma 0/0
-            CP
Internet 133.33.33.4   1  00:01:e8:d5:9e:e2  Ma 0/0
-            CP
```

Usage Information

The following describes the `show arp summary` command shown in the following example.

Row Heading	Description
Total Entries	Lists the total number of ARP entries in the ARP table.
Static Entries	Lists the total number of configured or static ARP entries.
Dynamic Entries	Lists the total number of learned or dynamic ARP entries.

Row Heading	Description
CPU	Lists which CPU the entries are stored on.

Example (Summary)

```
#show arp summary

TotalEntries Static Entries Dynamic Entries CPU
----------------------------------------------
3             0               3           CP
Dell
```

Related Commands

ip local-proxy-arp — enables/disables Layer 3 communication in secondary VLANs.

switchport mode private-vlan — sets PVLAN mode of the selected port.

show arp retries

Display the configured number of ARP retries.

Syntax `show arp retries`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on MXL 10/40GbE Switch IO Module

Related Commands

arp retries — sets the number of ARP retries in case the system does not receive an ARP reply in response to an ARP request.

show hosts

View the host table and DNS configuration.

Syntax `show hosts`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show hosts` command in the following example.

Field	Description
Default domain...	Displays the domain name (if configured).
Name/address lookup...	States if DNS is enabled on the system. • If DNS is enabled, the Name/Address lookup is domain service. • If DNS is not enabled, the Name/Address lookup is static mapping
Name servers are...	Lists the name servers, if configured.
Host	Displays the host name assigned to the IP address.
Flags	Classifies the entry as one of the following: • perm — the entry was manually configured and will not time out • temp — the entry was learned and will time out after 72 hours of inactivity. Also included in the flag is an indication of the validity of the route: • ok — the entry is valid. • ex — the entry expired. • ?? — the entry is suspect.
TTL	Displays the amount of time until the entry ages out of the cache. For dynamically learned entries only.
Type	Displays IP as the type of entry.
Address	Displays the IP addresses assigned to the host.

Example

```
Dell#show hosts
Default domain is not set
Name/address lookup uses static mappings
Name servers are not set
Host      Flags      TTL   Type   Address
--------- -----      ----  ----   -------
ks       (perm, OK)  -     IP     2.2.2.2
4200-1   (perm, OK)  -     IP     192.68.69.2
1230-3   (perm, OK)  -     IP     192.68.99.2
ZZr      (perm, OK)  -     IP     192.71.18.2
Z10-3    (perm, OK)  -     IP     192.71.23.1
Dell#
```

Related Commands

traceroute — views the DNS resolution.

ip host — configures a host.

show ip cam stack-unit

Display CAM entries.

Syntax

```
show ip cam stack-unit {0-5} [port-set {pipe-number} | {ip-
address mask [longer-prefixes]| detail | member-info | summary]
```

Parameters

0–5	Enter the stack-unit ID from 0 to 5
pipe-number	Enter the number of the Port-Pipe number. The range is from 0 to 0
ip-address mask [longer-prefixes]	(OPTIONAL) Enter the IP address and mask of a route to CAM entries for that route only. Enter the keywords `longer-prefixes` to view routes with a common prefix.
detail	Enter the keyword `detail` to display the group index ID used by the ecmp routes in the CAM.
member-info	Enter the keywords `member-info` to display the group index used by the ecmp, the number of egress ports (members) for the ecmp, and the port details of each member. The detail information under `member-info` gives the MAC address, VLAN ID, and gateway of every member port of the ecmp.
summary	(OPTIONAL) Enter the keyword `summary` to view a table listing route prefixes and the total number routes which can be entered in to CAM.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show ip cam` command shown in the following example.

Field	Description
Destination	Displays the destination route of the index.
EC	Displays the number of equal cost multipaths (ECMP) available for the default route for non-Jumbo line cards. For Jumbo line cards, displays 0,1 when ECMP is more than eight.
CG	Displays 0.
V	Displays a 1 if the entry is valid and a 0 otherwise.

Field	Description
C	Displays the CPU bit. 1 indicates that a packet hitting this entry is forwarded to the CP or RP2, depending on Egress port.
V Id	Displays the VLAN ID. If the entry is 0, the entry is not part of a VLAN.
Mac Addr	Displays the next-hop router's MAC address.
Port	Displays the egress interface. Use the second half of the entry to determine the interface. For example, in the entry 17cl CP, the CP is the pertinent portion. • CP = control processor • Gi = Gigabit Ethernet interface • Te = 10–Gigabit Ethernet interface

Example

```
Dell#show ip cam stack-unit 0 port-set 0 10.10.10.10/32 longer-
prefixes

Destination   EC CG V C VId  Mac-Addr           Port
----------------- -- -- - ------ --------------------
10.10.10.10   0 0 1 1 0    00:00:00:00:00:00  3f01 CP
Dell#
```

Usage Information

The following describes the `show ip cam ecmp-group` command shown in the following example.

Field	Description
Prefix Length	Displays the prefix-length or mask for the IP address configured on the linecard 0 port pipe 0.
Current Use	Displays the number of routes currently configured for the corresponding prefix or mask on the linecard 0 port pipe 0.
Initial Size	Displays the CAM size the system allocates for the corresponding mask. The system adjusts the CAM size if the number of routes for the mask exceeds the initial allocation.

Example (ECMP-Group)

```
Dell#show ip cam stack-unit 0 po 0 ecmp-group detail

Destination EC CG V C VId Mac-Addr        Port ECMP Group-Index
----------------- -- -- - ----- ---------------- -------------
1.1.1.2       0 0 1 0   0 00:01:e8:8a:d6:58    0004 Te 0/3    -
2.1.1.2       0 0 1 0   0 00:01:e8:8a:d6:58    0009 Te 0/8    -
1.1.1.1       0 0 1 1   0 00:00:00:00:00:00    3f01 CP        -
2.1.1.1       0 0 1 1   0 00:00:00:00:00:00    3f01 CP        -
1.1.1.0       0 0 1 1   0 00:00:00:00:00:00    3f01 CP        -
2.1.1.0       0 0 1 1   0 00:00:00:00:00:00    3f01 CP        -
100.1.1.      0 1 0 1   0 0 00:01:e8:8a:d6:58  0004 Te 0/3    0
100.1.1.      0 1 0 1   0 0 00:01:e8:8a:d6:58  0009 Te 0/8    0
0.0.0.0       0 0 1 1   0 00:00:00:00:00:00    3f01 CP        -
Dell#
```

Example (Member-Info)

```
Dell#show ip cam stack-unit 0 po 0 ecmp-group member-info
detail

Group Index Member Count  Mac-Addr      Port   VLan ID  Gateway
----------- ------------------------------- ------------------
  0                     2       00:01:e8:8a:d6:58  Te 0/3
0    1.1.1.2
                       00:01:e8:8a:d6:58  Te 0/8   0    2.1.1.2
Dell#
```

show ip fib stack-unit

View all FIB entries.

Syntax

`show ip fib stack-unit` *`0–5`* `[`*`ip-address`* `[`*`mask`*`] [longer-prefixes] | summary]`

Parameters

0–5	Enter the unit ID, from 0 to 5.
ip-address mask	(OPTIONAL) Enter the IP address of the network destination to view only information on that destination. Enter the IP address in dotted decimal format (A.B.C.D). Enter the mask in slash prefix format (/X).
longer-prefixes	(OPTIONAL) Enter the keywords `longer-prefixes` to view all routes with a common prefix.
summary	(OPTIONAL) Enter the keyword `summary` to view the total number of prefixes in the FIB.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show ip fib stack-unit` command shown in the following example.

Field	Description
Destination	Lists the destination IP address.
Gateway	Displays either the word “direct” and an interface for a directly connected route or the remote IP address used to forward the traffic.
First-Hop	Displays the first hop IP address.
Mac-Addr	Displays the MAC address.
Port	Displays the egress-port information.

Field	Description
VId	Displays the VLAN ID. If no VLAN is assigned, zero (0) is listed.
EC	Displays the number of ECMP paths.

Example

```
Dell#show ip fib stack-unit 0

Destination     Gateway       First-Hop     Mac-Addr
Port    VId EC
----------------------------------------------------------------
--------
10.10.10.10/32 Direct, Nu 0  0.0.0.0   00:00:00:00:00:00 BLK
HOLE 0 0

Dell>
```

Related Commands

clear ip fib stack-unit — clear FIB entries on a specified stack-unit.

show ip interface

View IP-related information on all interfaces.

Syntax

`show ip interface [interface | brief] [configured]`

Parameters

interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For a Loopback interface, enter the keyword `Loopback` then a number from 0 to 16383. • For the Management interface, enter the keyword `ManagementEthernet` then zero (0). • For the Null interface, enter the keyword `null` then zero (0). • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.
brief	(OPTIONAL) Enter the keyword `brief` to view a brief summary of the interfaces and whether an IP address is assigned.
configured	(OPTIONAL) Enter the keyword `configured` to display the physical interfaces with non-default configurations only.

Command Modes	- EXEC - EXEC Privilege
Command History	Version 8.3.16.1 — Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show ip interface` command shown in the following example.

Lines	Description
TenGigabitEthernet 0/0...	Displays the interface's type, slot/port, and physical and line protocol status.
Internet address...	States whether an IP address is assigned to the interface. If an IP address is assigned, that address is displayed.
IP MTU is...	Displays IP MTU value.
Inbound access...	Displays the name of the configured incoming access list. If none is configured, the phrase "not set" is displayed.
Proxy ARP...	States whether proxy ARP is enabled on the interface.
Split horizon...	States whether split horizon for RIP is enabled on the interface.
Poison Reverse...	States whether poison for RIP is enabled on the interface.
ICMP redirects...	States if ICMP redirects are sent.
ICMP unreachables...	States if ICMP unreachable messages are sent.

Example

```
Dell#show ip int te 0/0
TenGigabitEthernet 0/0 is down, line protocol is down
Internet address is not set
IP MTU is 1500 bytes
Inbound access list is not set
Proxy ARP is enabled
Split Horizon is enabled
Poison Reverse is disabled
ICMP redirects are not sent
ICMP unreachables are not sent

Dell#
```

Usage Information

The following describes the `show ip interface brief` command shown in the following example.

Fields	Description
Interface	Displays type of interface and the associated slot and port number.
IP-Address	Displays the IP address for the interface, if configured.
Ok?	Indicates if the hardware is functioning properly.

Fields	Description
Method	Displays “Manual” if the configuration is read from the saved configuration.
Status	States whether the interface is enabled (up) or disabled (administratively down).
Protocol	States whether IP is enabled (up) or disabled (down) on the interface.

Example (Brief)

```
Dell#show ip int brief
Interface            IP-Address  OK? Method
Status              Protocol
GigabitEthernet 1/0  unassigned  NO  Manual  administratively
down down
GigabitEthernet 1/1  unassigned  NO  Manual  administratively
down down
GigabitEthernet 1/2  unassigned  YES Manual
up                    up
GigabitEthernet 1/3  unassigned  YES Manual
up                    up
GigabitEthernet 1/4  unassigned  YES Manual
up                    up
GigabitEthernet 1/5  10.10.10.1  YES Manual
up                    up
GigabitEthernet 1/6  unassigned  NO  Manual  administratively
down down
```

show ip management-route

View the IP addresses assigned to the Management interface.

Syntax `show ip management-route [all | connected | summary | static]`

Parameters

all	(OPTIONAL) Enter the keyword `all` to view all IP addresses assigned to all Management interfaces on the switch.
connected	(OPTIONAL) Enter the keyword `connected` to view only routes directly connected to the Management interface.
summary	(OPTIONAL) Enter the keyword `summary` to view a table listing the number of active and non-active routes and their sources.
static	(OPTIONAL) Enter the keyword `static` to view non-active routes also.

Command Modes

- EXEC
- EXEC Privilege

Command History	**Version 8.3.16.1**	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show ip management-route

Destination     Gateway                    State
-----------     -------                    -----
10.1.2.0/24     ManagementEthernet 0/0     Connected
172.16.1.0/24   10.1.2.4                   Active
Dell#
```

show ip protocols

View information on all routing protocols enabled and active on the switch.

Syntax `show ip protocols`

Command Modes

- EXEC
- EXEC Privilege

Command History	**Version 8.3.16.1**	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show ip protocols
Routing Protocol is "bgp 1"
  Cluster Id is set to 20.20.20.3
  Router Id is set to 20.20.20.3
  Fast-external-fallover enabled
  Regular expression evaluation optimization enabled
  Capable of ROUTE_REFRESH
  For Address Family IPv4 Unicast
   BGP table version is 0, main routing table version 0
   Distance: external 20 internal 200 local 200
   Neighbor(s):
     Address : 20.20.20.2
     Filter-list in : foo
     Route-map in : foo
     Weight : 0
   Address : 5::6
     Weight : 0
Dell#
```

show ip route

View information, including how they were learned, about the IP routes on the switch.

Syntax `show ip route [`*`hostname`*` | `*`ip-address`*` [`*`mask`*`] [longer-prefixes] | list `*`prefix-list`*` [`*`process-id`*` | all | connected | static | summary]`

Parameters

ip-address	(OPTIONAL) Specify a name of a device or the IP address of the device to view more detailed information about the route.
mask	(OPTIONAL) Specify the network mask of the route. Use this parameter with the IP address parameter.
longer-prefixes	(OPTIONAL) Enter the keywords `longer-prefixes` to view all routes with a common prefix.
list *prefix-list*	(OPTIONAL) Enter the keyword `list` and the name of a configured prefix list. For more information, refer to the show ip route list command.
process-id	(OPTIONAL) Specify that only OSPF routes with a certain process ID must be displayed.
connected	(OPTIONAL) Enter the keyword `connected` to view only the directly connected routes.
all	(OPTIONAL) Enter the keyword `all` to view both active and non-active routes.
static	(OPTIONAL) Enter the keyword `static` to view only routes the `ip route` command configures.
summary	(OPTIONAL) Enter the keyword `summary`. For more information, refer to the show ip route summary command.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show ip route all` command in the following example.

Field	Description
(undefined)	Identifies the type of route: • C = connected • S = static • R = RIP • B = BGP • IN = internal BGP • EX = external BGP • LO = Locally Originated • O = OSPF • IA = OSPF inter area • N1 = OSPF NSSA external type 1

Field	Description
	• N2 = OSPF NSSA external type 2 • E1 = OSPF external type 1 • E2 = OSPF external type 2 • i = IS-IS • L1 = IS-IS level-1 • L2 = IS-IS level-2 • IA = IS-IS inter-area • * = candidate default • > = non-active route • + = summary routes
Destination	Identifies the route’s destination IP address
Gateway	Identifies whether the route is directly connected and on which interface the route is configured.
Dist/Metric	Identifies if the route has a specified distance or metric.
Last Change	Identifies when the route was last changed or configured.

Example

```
Dell#show ip route all

Codes:C- connected, S - static, R - RIP
      B- BGP, IN - internal BGP, EX - external BGP, LO -
Locally Originated
      O- OSPF, IA - OSPF inter area N1 - OSPF NSSA external
type 1
      N2- OSPF NSSA external type 2, E1 - OSPF external type 1
      E2- OSPF external type 2, i - IS-IS, L1 - IS-IS level-1
      L2- IS-IS level-2, IA - IS-IS inter area, * - candidate
default
      >- non-active route + - summary route

Gateway of last resort is not set

     Destination     Gateway            Dist/Metric Last Change
----------- ------- ----------- -----------
R   3.0.0.0/8       via 100.10.10.10, So 2/8 120/1   00:07:12
                    via 101.10.10.10, So 2/9
    100.10.10.0/24  Direct, So 2/8           0/0     00:08:54
> R 100.10.10.0/24  Direct, So 2/8           120/0   00:08:54
C   101.10.10.0/24  Direct, So 2/9           0/0     00:09:15
> R 101.10.10.0/24  Direct, So 2/9           120/0   00:09:15
Dell#
```

Example (Summary)

```
Dell#show ip route summary

Route Source  Active Routes   Non-active Routes
connected     2               0
static        1               0
Total         3               0
Total 3 active route(s) using 612 bytes
R1_E600i>show ip route static ?
|                    Pipe through a command
<cr>
R1_E600i>show ip route static
```

```
    Destination   Gateway            Dist/Metric Last Change
----------- -------- ----------- -----------
*S  0.0.0.0/0     via 10.10.91.9, Gi 1/2     1/0        3d2h
Dell>
```

show ip route list

Display IP routes in an IP prefix list.

Syntax

`show ip route list` *`prefix-list`*

Parameters

prefix-list	Enter the name of a configured prefix list.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show ip route list test

Codes:C- connected, S - static, R - RIP,
      B- BGP, IN - internal BGP, EX - external BGP,LO -
Locally Originated,
      O- OSPF, IA - OSPF inter area, N1 - OSPF NSSA external
type 1,
      N2- OSPF NSSA external type 2, E1 - OSPF external type 1,
      E2- OSPF external type 2, i - IS-IS, L1 - IS-IS level-1,
      L2- IS-IS level-2, IA - IS-IS inter area, * - candidate
default,
      >- non-active route, + - summary route

Gateway of last resort is not set

    Destination   Gateway             Dist/Metric Last Change
    -----------   -------             ----------- -----------
R   2.1.0.0/24   via 2.1.4.1, Gi 4/43   120/2       3d0h
R   2.1.1.0/24   via 2.1.4.1, Gi 4/43   120/2       3d1h
R   2.1.2.0/24   via 2.1.4.1, Gi 4/43   120/1       3d0h
R   2.1.3.0/24   via 2.1.4.1, Gi 4/43   120/1       3d1h
C   2.1.4.0/24   Direct, Gi 4/43          0/0       3d1h
```

Related Commands

ip prefix-list — enters CONFIGURATION-IP PREFIX-LIST mode and configures a prefix list.

show ip prefix-list summary — displays a summary of the configured prefix lists.

show ip route summary

View a table summarizing the IP routes in the switch.

Syntax `show ip route summary`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show ip route summary` shown in the following example.

Column Heading	Description
Route Source	Identifies how the route is configured in the system.
Active Routes	Identifies the best route if a route is learned from two protocol sources.
Non-active Routes	Identifies the back-up routes when a route is learned by two different protocols. If the best route or active route goes down, the non-active route becomes the best route.
ospf 100	If routing protocols (OSPF, RIP) are configured and routes are advertised, then information on those routes is displayed.
Total 1388 active...	Displays the number of active and non-active routes and the memory usage of those routes. If there are no routes configured in the the system, this line does not appear.

Example

```
Dell>show ip route summary

Route Source   Active Routes   Non-active Routes
connected      17              0
static         3               0
ospf 100       1368            2
Intra-area: 762 Inter-area: 1 External-1: 600 External-2: 5
Total          1388            2
Total 1388 active route(s) using 222440 bytes
Total 2 non-active route(s) using 128 bytes
Dell>
```

Related Commands

show ip route — displays information about the routes found in the switch.

show ip traffic

View IP, ICMP, UDP, TCP and ARP traffic statistics.

Syntax	`show ip traffic`
Command Modes	EXEC Privilege
Command History	Version 8.3.16.1 — Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show ip traffic` summary shown in the following example.

Keyword	Definition
unknown protocol...	No receiver for these packets. Counts packets whose protocol type field is not recognized by the system.
not a gateway...	Packets can not be routed; the host/network is unreachable.
security failures...	Counts the number of received unicast/multicast packets that could not be forwarded due to: • route not found for unicast/multicast; ingress interfaces do not belong to the destination multicast group • destination IP address belongs to reserved prefixes; the host/network is unreachable
bad options...	Unrecognized IP option on a received packet.
Frags:	IP fragments received.
... reassembled	Number of IP fragments that were reassembled.
... timeouts	Number of times a timer expired on a reassembled queue.
... too big	Number of invalid IP fragments received.
... couldn’t fragment	Number of packets that could not be fragmented and forwarded.
...encapsulation failed	Counts packets which could not be forwarded due to ARP resolution failure. The system sends an arp request prior to forwarding an IP packet. If a reply is not received, the system repeats the request three times. These packets are counted in encapsulation failed.
Rcvd:	
...short packets	The number of bytes in the packet are too small.
...bad length	The length of the packet was not correct.
...no port broadcasts	The incoming broadcast/multicast packet did not have any listener.

Keyword	Definition
...socket full	The applications buffer is full and the incoming packet are dropped.

The F10 Monitoring MIB provides access to the following statistics.

- **IP Statistics: Bcast: Received:** Object = f10BcastPktRecv, OIDs = 1.3.6.1.4.1.6027.3.3.5.1.1
- **IP Statistics: Bcast: Sent:** Object = f10BcastPktSent, OIDs = 1.3.6.1.4.1.6027.3.3.5.1.2
- **IP Statistics: Mcast: Received:** Object = f10McastPktRecv, OIDs = 1.3.6.1.4.1.6027.3.3.5.1.3
- **IP Statistics: Mcast: Sent:** Object = f10McastPktSent, OIDs = 1.3.6.1.4.1.6027.3.3.5.1.4
- **ARP Statistics: Rcvd: Request:** Object = f10ArpReqRecv, OIDs = 1.3.6.1.4.1.6027.3.3.5.2.1
- **ARP Statistics: Rcvd: Replies:** Object = f10ArpReplyRecv, OIDs = 1.3.6.1.4.1.6027.3.3.5.2.3
- **ARP Statistics: Sent: Request:** Object = f10ArpReqSent, OIDs = 1.3.6.1.4.1.6027.3.3.5.2.2
- **ARP Statistics: Sent: Replies:** Object = f10ArpReplySent, OIDs = 1.3.6.1.4.1.6027.3.3.5.2.4
- **ARP Statistics: Sent: Proxy:** Object = f10ArpProxySent, OIDs = 1.3.6.1.4.1.6027.3.3.5.2.5

Example

```
Dell#show ip traffic
IP statistics:
  Rcvd: 10021161 total, 3197480 local destination
    2501 format errors, 390 checksum errors, 0 bad hop count
    0 unknown protocol, 0 not a gateway
    115 security failures, 0 bad options
  Frags: 0 reassembled, 0 timeouts, 0 too big
    0 fragmented, 0 couldn't fragment
  Bcast: 6281 received, 0 sent; Mcast: 500 received, 0 sent
  Sent: 6573260 generated, 0 forwarded
    3830 encapsulation failed, 0 no route

ICMP statistics:
  Rcvd: 0 format errors, 0 checksum errors, 0 redirects, 3
unreachable
    0 echo, 0 echo reply, 0 mask requests, 0 mask replies, 0
quench
    0 parameter, 0 timestamp, 0 info request, 0 other
  Sent: 0 redirects, 1 unreachable, 0 echo, 0 echo reply
    0 mask requests, 0 mask replies, 0 quench, 0 timestamp
    0 info reply, 0 time exceeded, 0 parameter problem

UDP statistics:
  Rcvd: 2938110 total, 14 checksum errors, 1 no port
    0 short packets, 0 bad length, 1883908 no port broadcasts,
0 socket full
  Sent: 329731 total, 1883908 forwarded broadcasts
--More--
```

show tcp statistics

View information on TCP traffic through the switch.

Syntax `show tcp statistics`

Command Modes EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information The following describes the `show tcp statistics cp` command shown in the following example.

Field	Description
Rcvd:	Displays the number and types of TCP packets received by the switch. • Total = total packets received • no port = number of packets received with no designated port
0 checksum error...	Displays the number of packets received with the following: • checksum errors • bad offset to data • too short
329 packets...	Displays the number of packets and bytes received in sequence.
17 dup...	Displays the number of duplicate packets and bytes received.
0 partially...	Displays the number of partially duplicated packets and bytes received.
7 out-of-order...	Displays the number of packets and bytes received out of order.
0 packets with data after window	Displays the number of packets and bytes received that exceed the switch’s window size.
0 packets after close	Displays the number of packet received after the TCP connection was closed.
0 window probe packets...	Displays the number of window probe and update packets received.
41 dup ack...	Displays the number of duplicate acknowledgement packets and acknowledgement packets with data received.
10184 ack...	Displays the number of acknowledgement packets and bytes received.

Field	Description
Sent:	Displays the total number of TCP packets sent and the number of urgent packets sent.
25 control packets...	Displays the number of control packets sent and the number retransmitted.
11603 data packets...	Displays the number of data packets sent.
24 data packets retransmitted	Displays the number of data packets resent.
355 ack..	Displays the number of acknowledgement packets sent and the number of packet delayed.
0 window probe...	Displays the number of window probe and update packets sent.
7 Connections initiated...	Displays the number of TCP connections initiated, accepted, and established.
14 Connections closed...	Displays the number of TCP connections closed, dropped.
20 Total rxmt...	Displays the number of times the switch tried to re-send data and the number of connections dropped during the TCP retransmit timeout period.
0 Keepalive....	Lists the number of keepalive packets in timeout, the number keepalive probes and the number of TCP connections dropped during keepalive.

Example

```
Dell#show tcp statistics

Rcvd: 9849 Total, 0 no port
    0 checksum error, 0 bad offset, 0 too short
    5735 packets (7919 bytes) in sequence
    20 dup packets (2 bytes)
    0 partially dup packets (0 bytes)
    1 out-of-order packets (0 bytes)
    0 packets ( 0 bytes) with data after window
    0 packets after close
    0 window probe packets, 0 window update packets
    0 dup ack packets, 0 ack packets with unsend data
    6671 ack packets (152813 bytes)
Sent: 6778 Total, 0 urgent packets
    7 control packets
    6674 data packets (152822 bytes)
    12 data packets (1222 bytes) retransmitted
    85 ack only packets (5677 delayed)
    0 window probe packets, 0 window update packets
    0 Connections initiated, 7 connections accepted, 7
connections established
    8 Connections closed (including 4 dropped, 0 embryonic
dropped)
    12 Total rxmt timeout, 1 connections dropped in rxmt
timeout
    26 Keepalive timeout, 25 keepalive probe, 1 Connections
```

```
dropped in keepalive
Dell#
```

Related Commands

show ip cam stack-unit — displays the CAM table.

23

Internet Protocol Security (IPSec)

Internet protocol security (IPSec) is an end-to-end security scheme for securing IP communications by authenticating and encrypting all packets in a session. Use IPSec between hosts, gateways, or hosts and gateways.

IPSec uses a series of protocol functions to achieve information security:

- **Authentication Headers (AH)** — Connectionless integrity and origin authentication for IP packets.
- **Encapsulating Security Payloads (ESP)** — Confidentiality, authentication, and data integrity for IP packets.
- **Security Associations (SA)** — Algorithm-provided parameters required for AH and ESP protocols.

IPSec capability is available on control (protocol) and management traffic; end-node support is required.

IPSec supports two operational modes: Transport and Tunnel.

- Transport is the default mode for IPSec and encrypts only the payload of the packet. Routing information is unchanged.
- Tunnel mode is used to encrypt the entire packet, including the routing information in the IP header. Tunnel mode is typically used in creating virtual private networks (VPNs).

Transport mode provides IP packet payload protection using ESP. You can use ESP alone or in combination with AH to provide additional authentication. AH protects data from modification but does not provide confidentiality.

SA is the configuration information that specifies the type of security provided to the IPSec flow. The SA is a set of algorithms and keys used to authenticate and encrypt the traffic flow. The AH and ESP use SA to provide traffic protection for the IPSec flow.

NOTE:
Due to performance limitations on the control processor, you cannot enable IPSec on all packets in a communication session.

crypto ipsec transform-set

Create a transform set, or combination of security algorithms and protocols, of cryptos.

Syntax	`crypto ipsec transform-set` *`name`* `{ah-authentication {md5|sha1|null}	esp-authentication {md5|sha1|null}	esp-encryption {3des|cbc|des|null}}` To delete a transform set, use the `no crypto ipsec transform-set` *`name`* `{ah-authentication {md5|sha1|null}	esp-authentication {md5|sha1|null}	esp-encryption {3des|cbc|des|null}}` command.

Parameters

name	Enter the name for the transform set.
ah-authentication	Enter the keywords `ah-authentication` then the transform type of operation to apply to traffic. The transform type represents the encryption or authentication applied to traffic. • md5 — Use Message Digest 5 (MD5) authentication. • sha1 — Use Secure Hash Algorithm 1 (SHA-1) authentication. • null — Causes an encryption policy configured for the area to not be inherited on the interface.
esp-authentication	Enter the keywords `esp-authentication` then the transform type of operation to apply to traffic. The transform type represents the encryption or authentication applied to traffic. • md5 — Use Message Digest 5 (MD5) authentication. • sha1 — Use Secure Hash Algorithm 1 (SHA-1) authentication. • null — Causes an encryption policy configured for the area to not be inherited on the interface.
esp-encryption	Enter the keywords `esp-encryption` then the transform type of operation to apply to traffic. The transform type represents the encryption or authentication applied to traffic. • 3des — Use 3DES encryption. • cbc — Use CDC encryption. • des — Use DES encryption. • null — Causes an encryption policy configured for the area to not be inherited on the interface.

Defaults

none

Command Modes

CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

- Both sides of the link must specify the same transform set.
- You can create up to 64 transform sets.

Example

```
Dell(conf)#int ten 0/4
Dell(conf-if-te-0/4)#ipv6 address 200:1::/64 eui64
Dell(conf)#int ten 0/6
Dell(conf-if-te-0/6)#ipv6 address 801:10::/64 eui64
```

crypto ipsec policy

Create a crypto policy used by ipsec.

Syntax `crypto ipsec policy` *`name seq-num`* `ipsec-manual`

To delete a crypto policy entry, use the `no crypto ipsec policy` *`name seq-num`* `ipsec-manual` command.

Parameters

name	Enter the name for the crypto policy set.
seq-num	Enter the sequence number assigned to the crypto policy entry.

Defaults none

Command Modes CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information This command creates a crypto policy entry and enters the crypto policy configuration mode for configuring the flow parameters.

Example

```
Dell(conf)#crypto ipsec policy West 10 ipsec-manual
Dell(conf-crypto-policy)#
```

management crypto-policy

Apply the crypto policy to management traffic.

Syntax `management crypto-policy` *`name`*

To remove the management traffic crypto policy, use the `no management crypto-policy` *`name`* command.

Parameters

name	Enter the name for the crypto policy.

Defaults none

Command Modes CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

match

Match a sequence number to the transmission control protocol (TCP)/user datagram protocol (UDP) packets.

Syntax

`match` *`seq-num`* `{tcp | udp} {`*`ipv6`*` | `*`ip`*`}` *`port-num dest-ip dest-port-num`*

To remove the match filter for the crypto map, use the `no match` *`seq-num`* command.

Parameters

seq-num	Enter the match command sequence number. The range is from 0 to 255.
tcp	Enter the keyword `tcp` to configure a TCP access list filter.
udp	Enter the keyword `udp` to configure a UDP access list filter.
ipv6	Enter the source IPv6 address.
ip	Enter the source IPv4 address.
port-num	Enter the source port number. The range is from 0 to 65535
dest-ip	Enter the destination IP address.
dest-port-num	Enter the destination port number. The range is from 0 to 65535.

Defaults

none

Command Modes

CONFIG-CRYPTO-POLICY

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

UDP is not supported. Only TCP 23 telnet and 21 FTP are supported.

Example

```
Dell(conf-crypto-policy)#match 0 tcp a::1 /128 0 a::2 /128 23
Dell(conf-crypto-policy)#match 1 tcp a::1 /128 23 a::2 /128 0
Dell(conf-crypto-policy)#match 2 tcp a::1 /128 0 a::2 /128 21
Dell(conf-crypto-policy)#match 3 tcp a::1 /128 21 a::2 /128 0
Dell(conf-crypto-policy)#match 4 tcp 1.1.1.1 /32 0 1.1.1.2 /32
23
Dell(conf-crypto-policy)#match 5 tcp 1.1.1.1 /32 23
1.1.1.2 /32 0
Dell(conf-crypto-policy)#match 6 tcp 1.1.1.1 /32 0 1.1.1.2 /32
21
Dell(conf-crypto-policy)#match 7 tcp 1.1.1.1 /32 21
1.1.1.2 /32 0
```

session-key

Specify the session keys used in the crypto policy entry.

Syntax	`session-key {`*`inbound`*`	`*`outbound`*`} {`*`ah spi hex-key-string`*`	`*`esp spi encrypt hex-key-string auth hex-key-string`* To delete the session key information from the crypto policy, use the `no session-key {`*`inbound`*`	`*`outbound`*`} {`*`ah`*`	`*`esp`*`}` command.

Parameters

name	Enter the name of the host to delete. Enter * to delete all host table entries.
inbound	Specify the inbound session key for IPSec.
outbound	Specify the outbound session key for IPSec.
ah	Use the AH protocol when you select the AH transform set in the crypto policy.
esp	Use the ESP protocol when you select the ESP transform set in the crypto policy.
spi	Enter the security parameter index number.
hex-key-string	Enter the session key in hex format (a string of 8, 16, or 20 bytes). For DES algorithms, specify at least 16 bytes per key. For SHA algorithms, specify at least 20 bytes per key.
encrypt	Indicates the ESP encryption transform set key string.
auth	Indicates the ESP authentication transform set key string.

Defaults	none
Command Modes	CONF-CRYPTO-POLICY

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

- This command is only available in the ipsec-manual model.
- The key information entry is associated with the global method for enabling clear text or encrypted display in the running config.

show crypto ipsec transform-set

Display the transform set configuration.

Syntax `show crypto ipsec transform-set `*`name`*

Parameters	*name* Enter the name of the transform set.
Command Modes	EXEC
Command History	Version 9.2(0.2) Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell(conf)#do show crypto ipsec transform-set
Transform-Set Name    : ts1
Transform-Set refCnt  : 0
AH Transform          : md5
ESP Auth Transform    :
ESP Encry Transform   :
Dell(conf)#
```

show crypto ipsec policy

Display the crypto policy configuration.

Syntax

```
show crypto ipsec policy name
```

Parameters	*name* Enter the name for the crypto policy set.
Command Modes	EXEC
Command History	Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show crypto ipsec policy

Policy name           : West
Policy refcount       : 1
Sequence Num          : 10
SA Mode               : IPSEC-MANUAL
Transform-Set Name    : dallas
Peer IP Address       :
Inbound AH SPI        : 0
Inbound ESP Auth SPI  : 0
Inbound ESP Encry SPI : 256
Inbound AH Key        : [0]::
Inbound ESP Auth Key  : [0]::
Inbound ESP Encry Key :
[96]::a5b6b42009d47895b420a5b6789509d4b420a5b6789509d4b420a5b67
89509d4b420a5b6789509d4b420a5b6789509d4
Outbound AH SPI       : 0
Outbound ESP Auth SPI : 0
Outbound ESP Encry SPI: 257
Outound AH Key        : [0]::
Outound ESP Auth Key  : [0]::
Outound ESP Encry Key :
[96]::a5b6b42009d47895b420a5b6789509d4b420a5b6789509d4b420a5b67
89509d4b420a5b6789509d4b420a5b6789509d4
```

```
  Match sequence Num    : 0
  Protocol type         : tcp
  IP or IPv6            : IPv6
  Source address        : a::1
  Source mask           : /128
  Source port           : 0
  Destination address   : a::2
  Destination mask      : /128
  Destination port      : 23
  source-interface name :
  source-interface num  :


  Match sequence Num    : 1
  Protocol type         : tcp
  IP or IPv6            : IPv6
  Source address        : a::1
  Source mask           : /128
  Source port           : 23
  Destination address   : a::2
  Destination mask      : /128
  Destination port      : 0
  source-interface name :
  source-interface num  :


  Match sequence Num    : 2
  Protocol type         : tcp
  IP or IPv6            : IPv6
  Source address        : a::1
  Source mask           : /128
  Source port           : 0
  Destination address   : a::2
  Destination mask      : /128
  Destination port      : 21
  source-interface name :
  source-interface num  :


  Match sequence Num    : 3
  Protocol type         : tcp
  IP or IPv6            : IPv6
  Source address        : a::1
  Source mask           : /128
  Source port           : 21
  Destination address   : a::2
  Destination mask      : /128
  Destination port      : 0
  source-interface name :
  source-interface num  :

Dell#
```

transform-set

Specify the transform set the crypto policy uses.

Syntax	`transform-set` *`transform-set-name`* To delete a transform set from the crypto policy, use the `no transform-set` *`transform-set-name`* command.
Parameters	

transform-set-name	Enter the name for the crypto policy transform set.

Defaults	none
Command Modes	CONFIG-CRYPTO-POLICY
Command History	

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

24

IPv6 Access Control Lists (IPv6 ACLs)

IPv6 ACLs and IPv6 Route Map commands are supported on Dell Networking MXL switch.

NOTE: For IPv4 ACL commands, refer to the Access Control Lists (ACL) chapter.

Important Points to Remember

- Certain platforms require manual CAM usage space allotment. For more information, refer to the cam-acl (Configuration) command.
- Egress IPv6 ACL and IPv6 ACL on the Loopback interface is not supported.
- Reference to an empty ACL permits any traffic.
- ACLs are not applied to self-originated traffic (for example, Control Protocol traffic not affected by IPv6 ACL because the routed bit is not set for Control Protocol traffic and for egress ACLs the routed bit must be set).
- You can use the same access list name for both IPv4 and IPv6 ACLs.
- You can apply both IPv4 and IPv6 ACLs on an interface at the same time.
- You can apply IPv6 ACLs on physical interfaces and a logical interfaces (Port-channel/VLAN).
- Non-contiguous masks are not supported in source or destination addresses in IPv6 ACL entries.
- Because the prefix mask is specified in /x format in IPv6 ACLs, inverse mask is not supported.

IPv6 ACL Commands

The following commands configure IPv6 ACLs.

cam-acl

Allocate space for IPv6 ACLs.

Syntax

```
cam-acl {default | l2acl 1-10 ipv4acl 1-10 ipv6acl 0-10 ipv4qos
1-10 l2qos 1-10}
```

Parameters

default	Use the default CAM profile settings, and set the CAM as follows: • L3 ACL (ipv4acl): **6** • L2 ACL(l2acl): **5**

- IPv6 L3 ACL (ipv6acl): **0**
- L3 QoS (ipv4qos): **1**
- L2 QoS (l2qos): **1**

l2acl *1-10* ipv4acl *1-10* ipv6acl *0-10* ipv4qos *1-10* l2qos *1-10*	Allocate space to support IPv6 ACLs. Enter all of the profiles and a range. Enter the CAM profile name then the amount to be allotted. The total space allocated must equal 13. The `ipv6acl` range must be a factor of 2.

Command Modes

CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

For the new settings to take effect, save the new CAM settings to the startup-config (`write-mem` or `copy run start`), then reload the system.

The total amount of space allowed is 16 FP blocks. System flow requires three blocks and these blocks cannot be reallocated.

When configuring space for IPv6 ACLs, the total number of Blocks must equal 13.

Ranges for the CAM profiles are from 1 to 10, except for the `ipv6acl profile` which is from 0 to 10. The ipv6acl allocation must be a factor of 2 (2, 4, 6, 8, 10).

cam-acl-egress

Allocate space for IPv6 egress ACLs.

Syntax

`cam-acl-egress {default | l2acl` *`1-4`* `ipv4acl` *`1-4`* `ipv6acl` *`0-4`*`}`

Parameters

default	Use the default CAM profile settings, and set the CAM as follows: • L2 ACL(l2acl): **1** • L3 ACL (ipv4acl: **1** • IPv6 L3 ACL (ipv6acl): **2**
l2acl *1-4* ipv4acl *1- 4* ipv6acl *0-4*	Allocate space to support IPv6 ACLs. Enter all of the profiles and a range. Enter the CAM profile name then the amount to be allotted. The total space allocated must equal 13. The `ipv6acl` range must be a factor of 2.

Command Modes

CONFIGURATION

Command History	**Version 9.2(0.0)**	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

For the new settings to take effect, save the new CAM settings to the startup-config (`write-mem` or `copy run start`), then reload the system.

The total amount of space allowed is 16 FP Blocks. System flow requires three blocks and these blocks cannot be reallocated.

When configuring space for IPv6 ACLs, the total number of Blocks must equal 13.

Ranges for the CAM profiles are from 1 to 10, except for the `ipv6acl profile` which is from 0 to 10. The ipv6acl allocation must be a factor of 2 (2, 4, 6, 8, 10).

Example

```
Dell#
Dell#configure
Dell(conf)#cam-acl-egress ?
default      Reset Egress CAM ACL entries to default setting
l2acl        Set L2-ACL entries
Dell(conf)#cam-acl-egress l2acl ?
<1-4>        Number of FP blocks for l2acl
Dell(conf)#cam-acl-egress l2acl 1 ?
ipv4acl      Set IPV4-ACL entries
Dell(conf)#cam-acl-egress l2acl 1 ipv4acl 1 ?
ipv6acl      Set IPV6-ACL entries
Dell(conf)#cam-acl-egress l2acl 1 ipv4acl 1 ipv6acl ?
<0-4>        Number of FP blocks for IPV6 (multiples of 2)
Dell(conf)#cam-acl-egress l2acl 1 ipv4acl 1 ipv6acl 2
```

ipv6 access-list

Configure an access list based on IPv6 addresses or protocols.

Syntax

`ipv6 access-list` *`access-list-name`* `cpu-qos {permit | deny} ospfv3`

To delete an access list, use the `no ipv6 access-list` *`access-list-name`* command.

w

Parameters

access-list-name	Enter the access list name as a string, up to 140 characters.
cpu-qos	Enter the keyword `cpu-qos` to assign this ACL to control plane traffic only (CoPP).
permit	Enter the keyword `permit` to configure a filter to forward packets meeting this condition.
deny	Enter the keyword `deny` to configure a filter to drop packets meeting this condition.

ospfv3	Specify that this ACL is for OSPFv3 control plane traffic

Defaults	All access lists contain an implicit “deny any”; that is, if no match occurs, the packet is dropped.
Command Modes	CONFIGURATION
Command History	**Version 9.4(0.0)** Added support for CoPP for OSPFv3 on the MXL 10/40GbE Switch IO Module. **Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	The number of entries allowed per ACL is hardware-dependent. For detailed specification on entries allowed per ACL, refer to your line card documentation. You can create an IPv6 ACL for control-plane traffic policing for OSPFv3, in addition to the CoPP support for VRRP, BGP, and ICMP that existed in Dell Networking OS releases 9.3(0.0) and earlier
Related Commands	show config — views the current configuration.

ipv6 control-plane egress-filter

Enable egress Layer 3 ACL lookup for IPv6 CPU traffic.

Syntax	`ipv6 control-plane egress-filter`
Defaults	Not enabled.
Command Modes	EXEC Privilege
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.

permit

To configure a filter that matches the filter criteria, select an IPv6 protocol number, ICMP, IPv6, TCP, or UDP.

Syntax

```
permit {ipv6-protocol-number | icmp | ipv6 | tcp | udp} [count
[byte]] [dscp value] [order] [fragments] [log [interval
minutes] [threshold-in-msgs [count]] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command syntax if you know the filter’s sequence number

- Use the `no permit {ipv6-protocol-number | icmp | ipv6 | tcp | udp}` command

Parameters

ip-protocol-number	Enter an IPv6 protocol number. The range is from 0 to 255.
icmp	Enter the keyword `icmp` to filter internet Control Message Protocol version 6.
ipv6	Enter the keyword `ipv6` to filter any internet Protocol version 6.
tcp	Enter the keyword `tcp` to filter the Transmission Control protocol.
udp	Enter the keyword `udp` to filter the User Datagram Protocol.
count	(OPTIONAL) Enter the keyword `count` to count packets the filter processes.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes the filter processes.
dscp	(OPTIONAL) Enter the keyword `dcsp` to match to the IP DCSCP values.
order	(OPTIONAL) Enter the keyword order to specify the QoS priority for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). If you do not use the keyword `order`, the ACLs have the lowest order by default (**255**).
fragments	Enter the keyword `fragments` to use ACLs to control packet fragments.
log	OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
threshold-in-*msgs*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the `keyword` interval followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

Not configured.

Command Modes	ACCESS-LIST

Command History

Version 9.4(0.0)	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module.
Version 9.3(0.0)	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module.
Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

permit icmp

To allow all or specific internet control message protocol (ICMP) messages, configure a filter.

Syntax

`permit icmp {`*`source address mask`*` | any | host `*`ipv6-address`*`} {`*`destination address`*` | any | host `*`ipv6-address`*`} [`*`message-type`*`] [count [byte]] | [log] [interval minutes] [threshold-in-msgs [`*`count`*`]][monitor]`

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no permit icmp {`*`source address mask`*` | any | host `*`ipv6-address`*`} {`*`destination address`*` | any | host `*`ipv6-address`*`}` command.

Parameters

source address	Enter the IPv6 address of the network or host from which the packets were sent in the x:x:x:x::x format then the prefix length in the /x format. The range is from /0 to /128. The :: notation specifies successive hexadecimal fields of zero.
mask	Enter a network mask in /prefix format (/x).
any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ipv6-address*	Enter the keyword `host` then the IPv6 address of the host in the x:x:x:x::x format. The :: notation specifies successive hexadecimal fields of zero.
destination address	Enter the IPv6 address of the network or host to which the packets are sent in the x:x:x:x::x format then the prefix length in the /x format. The range is from /0 to /128. The :: notation specifies successive hexadecimal fields of zero.
message-type	(OPTIONAL) Enter an ICMP message type, either with the type (and code, if necessary) numbers or with the name of the message type. The range is from 0 to 255 for ICMP type and from 0 to 255 for ICMP code.

count	(OPTIONAL) Enter the keyword `count` to count packets the filter processes.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes the filter processes.
log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
threshold-in-msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

ACCESS-LIST

Command History

Version 9.4(0.0)	Added the support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform
Version 9.3(0.0)	Added the support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform
Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module platform.

Usage Information

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

show cam-acl

Show space allocated for IPv6 ACLs.

Syntax

```
show cam-acl
```

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
show cam-acl (non default)
Dell(conf)#cam-acl l2acl 2 ipv4acl 4 ipv6acl 4 ipv4qos 2 l2qos
1 l2pt 0 ipmacacl 0 vman-qos 0 ecfmacl  0
Dell#show cam-acl

-- Chassis Cam ACL --
             Current Settings(in block sizes)
                   1 block = 128 entries
L2Acl        :        2
Ipv4Acl      :        4
Ipv6Acl      :        4
Ipv4Qos      :        2
L2Qos        :        1
L2PT         :        0
IpMacAcl     :        0
VmanQos      :        0
VmanDualQos  :        0
EcfmAcl      :        0
FcoeAcl      :        0
iscsiOptAcl  :        0
ipv4pbr      :        0
vrfv4Acl     :        0
Openflow     :        0
fedgovacl    :        F3940

-- stack-unit 0 --
           Current Settings(in block sizes)
                   1 block = 128 entries
L2Acl        :        2
Ipv4Acl      :        4
Ipv6Acl      :        4
Ipv4Qos      :        2
```

```
L2Qos          :         1
L2PT           :         0+F394
IpMacAcl       :         0
VmanQos        :         0
VmanDualQos    :         0
EcfmAcl        :         0
FcoeAcl        :         0
iscsiOptAcl    :         0
ipv4pbr        :         0
vrfv4Acl       :         0
Openflow       :         0
fedgovacl      :         0

Dell#
```

Related Commands

cam-acl — configures CAM profiles to support IPv6 ACLs.

show cam-acl-egress

Show information on FP groups allocated for egress ACLs.

Syntax

`show cam-acl-egress`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show cam-acl-egress

-- Chassis Egress Cam ACL --
             Current Settings(in block sizes)
                   1 block = 256 entries
L2Acl          :         1
Ipv4Acl        :         1
Ipv6Acl        :         2

-- stack-unit 0 --
           Current Settings(in block sizes)
L2Acl          :         1
Ipv4Acl        :         1
Ipv6Acl        :         2
```

Related Commands

cam-acl — configures CAM profiles to support IPv6 ACLs.

25

IPv6 Basics

This chapter describes IPv6 basic commands for the MXL 10/40GbE Switch IO Module.

clear ipv6 fib

Clear (refresh) all forwarding information base (FIB) entries on a linecard or stack unit.

Syntax `clear ipv6 fib linecard slot | stack-unit unit-number`

Parameters

slot	Enter the slot number to clear the FIB for a linecard.
unit-number	Enter the stack member number.

Command Modes EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

clear ipv6 route

Clear (refresh) all or a specific route from the IPv6 routing table.

Syntax `clear ipv6 route {* | ipv6-address prefix-length}`

Parameters

*	Enter the `*` to clear (refresh) all routes from the IPv6 routing table.
ipv6-address prefix-length	Enter the IPv6 address in the x:x:x:x::x format then the prefix length in the /x format. The range is from /0 to /128. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.

Command Modes EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

clear ipv6 mld_host

Clear the IPv6 MLD host counters and reset the elapsed time.

Syntax	`clear ipv6 mld_host`
Command Modes	EXEC
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.

ipv6 address autoconfig

Configure IPv6 address auto-configuration for the management interface.

Syntax	`ipv6 address autoconfig` To disable the address autoconfig operation on the management interface, use the `no ipv6 address autoconfig` command.
Default	Disabled
Command Modes	INTERFACE (management interface only)
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.

Usage Infomation

- SAA can configure up to two addresses. If any preferred prefix or valid timers time out, the corresponding address are deprecated or removed. If an address is removed due to a time-out, an address from the current unused prefix is used to create a new address. If there are no remaining prefixes, the software waits to receive a new prefix from the RA.
- If auto-configuration is enabled, all IPv6 addresses on that management interface are auto-configured. Manual and auto-configurations are not supported on a single management interface.
- Removing auto-configuration removes all auto-configured IPv6 addresses and the link-local IPv6 address from that management interface.
- IPv6 addresses on a single management interface cannot be members of the same subnet.
- IPv6 secondary addresses on management interfaces across a platform must be members of the same subnet.
- IPv6 secondary addresses on management interfaces should not match the virtual IP address and should not be in the same subnet as the virtual IP.

ipv6 address

Configure an IPv6 address to an interface.

Syntax	`ipv6 address {`*`ipv6-address prefix-length`*`}` To remove the IPv6 address, use the `no ipv6 address {`*`ipv6-address prefix-length`*`}` command.
Parameters	*ipv6-address prefix-length*: Enter the IPv6 address in the x:x:x:x::x format then the prefix length in the /x format. The range is from /0 to /128. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
Defaults	none
Command Modes	INTERFACE
Command History	**Version 9.2(0.0)**: Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

- If two addresses are configured, delete an existing address before configuring a new address.
- If the last manually-configured global IPv6 address is removed using the "no" form of the command, the link-local IPv6 address is removed automatically.
- IPv6 addresses on a single management interface cannot be members of the same subnet.
- IPv6 secondary addresses on management interfaces across platform must be members of the same subnet.
- IPv6 secondary addresses on management interfaces should not match the virtual IP address and should not be in the same subnet as the virtual IP.

Example

```
Dell(conf)#interface tengigabitethernet x/x
Dell(conf-if-te-x/x)#ipv6 address ?
X:X:X:X::X IPv6 address
Dell(conf-if-te-x/x)#ipv6 address 2002:1:2::3 ?
<0-128> Prefix length in bits
Dell(conf-if-te-x/x)#ipv6 address 2002:1:2::3 /96 ?
Dell(conf-if-te-x/x)#ipv6 address 2002:1:2::3 /96
Dell(conf-if-te-x/x)#show config
```

ipv6 address eui64

Configure IPv6 EUI64 address configuration on the interface.

Syntax

`ipv6 address {ipv6-address prefix-length} eui64`

To disable IPv6 EUI64 address autoconfiguration, use the `no ipv6 address {ipv6-address prefix-length} eui64` command.

Parameters

ipv6-address prefix-length	Enter the IPv6 prefix in the x:x:x:x::x format then the prefix length in the /x format. The range is from /0 to /128. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.

Defaults

none

Command Modes

CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

This command allows you to create an EUI64 address based on the specified prefix and MAC address only. Prefixes may be configured on the interface using the `ipv6 nd prefix` command without creating an EUI64 address.

Example

```
Dell(conf)#int ten 0/4
Dell(conf-if-te-0/4)#ipv6 address 200:1::/64 eui64
Dell(conf)#int ten 0/6
Dell(conf-if-te-0/6)#ipv6 address 801:10::/64 eui64
```

ipv6 control-plane icmp error-rate-limit

Configure the maximum number of ICMP error packets per second that can be sent per second.

Syntax

`ipv6 control-plane icmp error-rate-limit {1-200}`

To restore the default value, use the `no ipv6 control-plane icmp error-rate-limit` command.

Parameters

pps	Enter the maximum number of error packets generated per second. The range is from 1 to 200, where 0 disables the rate-limiting.

Default

100 pps

Command Modes

CONFIGURATION

Command History	Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

ipv6 flowlabel-zero

Configure system to set the flow label field in the packets to zero.

Syntax

```
ipv6 flowlabel-zero
```

To disable the 0 from being set in the field and allow the rotocol operations to fill the field, use the `no ipv6 flowlabel-zero` command.

Default Disabled

Command Modes CONFIGURATION

Command History	Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information If the flowlabel value is already set for BGP or SSH, the system defaults to the already configured value. All packets on the same connection are considered part of the same flow by the system. For new connections, set the new flowlabel to zero.

ipv6 host

Assign a name and IPv6 address the host-to-IPv6 address mapping table uses.

Syntax

```
ipv6 host name ipv6-address
```

To remove an IP host, use the `no ipv6 host name {ipv6-address}`.

Parameters

name	Enter a text string to associate with one IP address.
ipv6-address	Enter the IPv6 address (X:X:X:X::X) to be mapped to the name.

Defaults Not configured.

Command Modes CONFIGURATION

Command History	Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

ipv6 name-server

Enter up to six IPv6 addresses of name servers. The order you enter the addresses determines the order of their use.

Syntax	`ipv6 name-server` *`ipv6-address`* `[`*`ipv6-address2... ipv6-address6`*`]` To remove a name server, use the `no ipv6 name—server ipv6–address` command.

Parameters

ipv6-address	Enter the IPv6 address (X:X:X:X::X) of the name server to be used. **NOTE:** The :: notation specifics successive hexadecimal fields of zeros.
ipv6-address2... ipv6-address6	(OPTIONAL) Enter up to five more IPv6 addresses, in the x:x:x:x::x format, of name servers to be used. Separate the IPv6 addresses with a space.

Defaults	none
Command Modes	CONFIGURATION
Command History	Version 9.2(0.0) — Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	You can separately configure both IPv4 and IPv6 domain name servers.

ipv6 nd dad attempts

To perform duplicate address detection (DAD) on the management interface, configure the number of neighbor solicitation messages that are sent.

Syntax	`ipv6 nd dad attempts {`*`number of attempts`*`}` To restore the default value, use the `no ipv6 nd dad attempts` command.

Parameters

number of attempts	Enter the number of attempts to be made to detect a duplicate address. The range is from 0 to 15. Setting the value to 0 disables DAD on the interface.

Default	3 attempts
Command Modes	INTERFACE (management interface only)

Command History	Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

ipv6 nd dns-server

Configures Recursive DNS Server (RDNSS) addresses to be distributed via IPv6 router advertisements to an IPv6 device.

Syntax

`ipv6 nd dns-server {ipv6-RDNSS-address} {lifetime | infinite}`

To remove the IPv6 RDSS configuration, use `no ipv6 nd dns-server {ipv6-RDNSS-address} {lifetime | infinite}`

Parameters

ipv6-RDNSS-address	Enter the IPv6 Recursive DNS Server's (RDNSS) address. You can specify up to 4 IPv6 RDNSS server addresses.
lifetime	Enter the lifetime in seconds. The amount of time the IPv6 host can use the IPv6 RDNSS address for name resolution. The range is `0` to `4294967295` seconds. When you specify the maximum lifetime value of `4294967295` or `infinite`, the lifetime does not expire. A value of `0` indicates to the host that the RDNSS address should not be used. You must specify a lifetime using the `lifetime` or `infinite` parameter.
infinite	Enter the keyword `infinite` to specify that the RDNSS lifetime does not expire.

Defaults Not Configured

Command Modes INTERFACE CONFIG

Command History

Version 9.5(0.0)	Added support for roles on the Z9000.
	Added support for roles on the S6000.
	Added support for roles on the S4820T.
	Added support for roles on the S4810.
	Added support for roles on the MXL.

Usage Information Use this command to add, edit, or delete an IPv6 RDNSS address and lifetime value. You can configure up to four IPv6 RDNSS addresses. You must specify a lifetime using the lifetime or infinite parameter.

Example Dell(conf-if-te-0/1)#ipv6 nd dns-server 1000::1 1

ipv6 nd prefix

Specify which IPv6 prefixes are included in Neighbor Advertisements.

Syntax

```
ipv6 nd prefix {ipv6-prefix | prefix-length | default} [no-
advertise] | [no-autoconfig] [no-rtr-address] [off-link]
[lifetime {valid | infinite} {preferred | infinite}]
```

Parameters

ipv6-prefix	Enter an IPv6 prefix.
prefix-length	Enter the prefix then the prefix length. The length range is from 0 to 128.
default	Enter the keyword `default` to set default parameters for all prefixes.
no-advertise	Enter the keyword `no-advertise` to prevent the specified prefix from being advertised.
no-autoconfig	Enter the keywords `no-autoconfig` to disable Stateless Address Autoconfiguration.
no-rtr-address	Enter the keyword `no-rtr-address` to exclude the full router address from router advertisements (the R bit is not set).
off-link	Enter the keywords `off-link` to advertise the prefix without stating to recipients that the prefix is either on-link or off-link.
valid-lifetime | infinite	Enter the amount of time that the prefix is advertised, or enter `infinite` for an unlimited amount of time. The range is from 0 to 4294967295. The default is **2592000**. The maximum value means that the preferred lifetime does not expire for the valid-life time parameter.
preferred-lifetime | infinite	Enter the amount of time that the prefix is preferred, or enter `infinite` for an unlimited amount of time. The range is from 0 to 4294967295. The default is **2592000**. The maximum value means that the preferred lifetime and does not expire.

Command Modes

INTERFACE

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

By default, all prefixes configured as addresses on the interface are advertised. This command allows control over the individual parameters per prefix; you can use the `default` keyword to use the default parameters for all prefixes. If a prefix has been configured with lifetime parameter values, the default values cannot be applied using the `ipv6 nd prefix default no-autoconfig` command.

ipv6 route

Establish a static IPv6 route.

Syntax	`ipv6 route ipv6-address prefix-length {ipv6-address | interface | interface ipv6-address} [distance] [tag value] [permanent]` To remove the IPv6 route, use the `no ipv6 route ipv6-address prefix-length {ipv6-address | interface | interface ipv6-address} [distance] [tag value] [permanent]` command.

Parameters

ipv6-address prefix-length	Enter the IPv6 address in the x:x:x:x::x format then the prefix length in the /x format. The range is from /0 to /128. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For a loopback interface, enter the keyword `loopback` then a number from zero (0) to 16383. • For the null interface, enter the keyword `null` then zero (0). • For a port channel interface, enter the keyword `port-channel` then the port channel number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a tunnel interface, enter the keyword `tunnel` then the tunnel interface number. The range is from 1 to 16383. • For a VLAN interface, enter the keyword `VLAN` then the vlan number. The range is from 1 to 4094. If you configure a static IPv6 route using an egress interface and enter the `ping` command to reach the destination IPv6 address, the ping operation may not work. Configure the IPv6 route using a next-hop IPv6 address in order for the `ping` command to detect the destination address.
ipv6-address	(OPTIONAL) Enter the forwarding router IPv6 address in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
distance	(OPTIONAL) Enter a number as the metric distance assigned to the route. The range is from 1 to 255.

tag *value*	(OPTIONAL) Enter the keyword `tag` then a tag value number. The range is from 1 to 4294967295.
permanent	(OPTIONAL) Enter the keyword `permanent` to specify that the route is not to be removed, even if the interface assigned to that route goes down. NOTE: If you disable the interface with an IPv6 address associated with the keyword `permanent`, the route disappears from the routing table.

Defaults

none

Command Modes

CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

When the interface goes down, the system withdraws the route. The route is re-installed by the system when the interface comes back up. When a recursive resolution is “broken,” the system withdraws the route. The route is re-installed by the system when the recursive resolution is satisfied.

After an IPv6 static route interface is created, if an IP address is not assigned to a peer interface, the peer must be manually pinged to resolve the neighbor information.

Example

```
Dell(conf)#ipv6 route ?
X:X:X:X::X              IPv6 prefix x:x::y
Dell(conf)#ipv6 route 44::0 ?
/nn                     /nn Mask in slash format
Dell(conf)#ipv6 route 44::0 /64 ?
X:X:X:X::X              Forwarding router's address
gigabitethernet         Gigabit Ethernet interface
loopback                Loopback interface
null                    Null interface
port-channel            Port-Channel interface
tenGigabitethernet      TenGigabit Ethernet interface
fortyGigE               FortyGigabit Ethernet interface
tunnel                  Tunnel interface
vlan                    Vlan interface
Dell(conf)#ipv6 route 44::0 /64 33::1 ?
<1-255>                 Distance metric for this route
permanent               Permanent route
tag                     Set tag for this route

Dell(conf)#ipv6 route 44::0 /64 33::1
Dell(conf)#ipv6 route 44::0 /64 tengigabitethernet 0/1 ?
X:X:X:X::X              Forwarding router's address
Dell(conf)#ipv6 route 44::0 /64 tengigabitethernet 0/1 66::1
Dell(conf)#
```

Related Commands

show ipv6 route — views the IPv6 configured routes.

ipv6 unicast-routing

Enable IPv6 Unicast routing.

Syntax

```
ipv6 unicast-routing
```

To disable unicast routing, use the `no ipv6 unicast-routing` command.

Defaults

Enabled

Command Modes

CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Because this command is enabled by default, it does not appear in the running configuration. When you disable unicast routing, the `no ipv6 unicast-routing` command is included in the running configuration. Whenever unicast routing is disabled or re-enabled, the system generates a syslog message indicating the action.

Disabling unicast routing on a chassis causes the following behavior:

- static and protocol learned routes are removed from RTM and from the CAM; packet forwarding to these routes is terminated
- connected routes and resolved neighbors remain in the CAM and new IPv6 neighbors are still discoverable
- additional protocol adjacencies (OSPFv3 and BGP4) are brought down and no new adjacencies are formed
- the IPv6 address family configuration (under router bgp) is deleted
- IPv6 Multicast traffic continues to flow unhindered

show ipv6 cam stack-unit

Displays the IPv6 CAM entries for the specified stack-unit.

Syntax

```
show ipv6 cam stack-unit unit-number port-set {0-1} [summary |
index | ipv6 address]
```

Parameters

unit-number	Enter the stack unit's ID number. The range is from 0 to 11.
port-set	Enter the keyword `Port Set`.
summary	(OPTIONAL) Enter the keyword `summary` to display a table listing network prefixes and the total number prefixes which can be entered into the IPv6 CAM.
index	(OPTIONAL) Enter the index in the IPv6 CAM.
ipv6-address	Enter the IPv6 address in the x:x:x:x::x/n format to display networks that have more specific prefixes. The range is from /0 to /128.

NOTE: The :: notation specifies successive hexadecimal fields of zeros.

Defaults	none
Command Modes	- EXEC - EXEC Privilege
Command History	Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

NOTE: If a route has a mask greater than 64, no output is displayed and no output is displayed for `show ipv6 cam stack-unit unit-number port-set {0-1} ipv6-address`, but an equivalent /64 entry would be listed in the `show ipv6 cam stack-unit unit-number port-set {0-1}` output. Similarly, if there is more than one ECMP object with a destination route that has a mask greater than 64, if the first 64 bits in the destination routes of the ECMP objects are the same, only one route is installed in CAM even though multiple ECMP path entries exist.

show ipv6 control-plane icmp

Displays the status of the icmp control-plane setting for the error eate limit setting.

Syntax	`show ipv6 control-plane icmp`
Default	100
Command Modes	EXEC
Command History	Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	ipv6 flowlabel-zero — Configure IPv6 address auto-configuration for the management interface.

show ipv6 fib stack-unit

View all FIB entries.

Syntax	`show ipv6 fib stack-unit` *`unit-number`* `[summary |` *`ipv6-address`*`]`
Parameters	*slot-number* Enter the number of the stack unit. The range is from 0 to 11.

summary	(OPTIONAL) Enter the keyword `summary` to view a summary of entries in IPv6 cam.
ipv6-address	Enter the IPv6 address in the x:x:x:x::x/n format to display networks that have more specific prefixes. The range is from /0 to /128. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Host tables are not stored in CAM tables. Entries for `camIndex` displays as zero (0) on the `show ipv6 fib stack-unit` output for neighbor entries, such as address resolution protocol (ARP) entries.

show ipv6 flowlabel-zero

Display the flow label zero setting.

Syntax

```
show ipv6 flowlabel-zero
```

Default

Disabled

Command Modes

EXEC

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

ipv6 nd dad attempts — Configure system to set the flow label field in the packets to zero.

show ipv6 interface

Display the status of interfaces configured for IPv6.

Syntax

```
show ipv6 interface interface [brief] [configured]
[gigabitethernet slot | slot/port] [linecard slot-number]
[loopback interface-number] [managementethernet slot/port]
[port-channel number] [tengigabitethernet slot | slot/port]
[fortyGigE slot | slot/port] [vlan vlan-id]
```

Parameters

interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For a Loopback interface, enter the keyword `Loopback` then a number from 0 to 16383. • For the Null interface, enter the keyword `null` then zero (0). • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For stacking, enter the keywords `stack-unit` then the stack-unit ID. • For a tunnel interface, enter the keyword `tunnel` then the tunnel ID. • For a VLAN interface, enter the keyword `VLAN`. • For a port channel interface, enter the keywords `port-channel`.
brief	(OPTIONAL) View a summary of IPv6 interfaces.
configured	(OPTIONAL) View information on all IPv6 configured interfaces.
gigabitethernet	(OPTIONAL) View information for an IPv6 gigabitethernet interface.
linecard *slot/port*	(OPTIONAL) View information for a specific IPv6 linecard or stack-unit. The range is 0 to 11.
managementethernet *slot/port*	(OPTIONAL) View information on an IPv6 Management port. Enter the slot number (0-1) and port number zero (0).
loopback	(OPTIONAL) View information for IPv6 Loopback interfaces.
port-channel	(OPTIONAL) View information for IPv6 port channels.
tengigabitethernet	(OPTIONAL) View information for an IPv6 tengigabitethernet interface.
fortyGigE	(OPTIONAL) View information for an IPv6 fortygigabitethernet interface.
vlan	(OPTIONAL) View information for IPv6 VLANs.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The Management port is enabled by default (`no shutdown`). If necessary, use the `ipv6 address` command to assign an IPv6 address to the Management port.

Example

```
Dell#show ipv6 int te 0/12
TenGigabitEthernet 0/12 is up, line protocol is up
  IPV6 is enabled
  Link Local address: fe80::201:e8ff:fea7:497e
  Global Unicast address(es):
    100::2, subnet is 100::/64 (MANUAL)
     Remaining lifetime: infinite
  Global Anycast address(es):
  Joined Group address(es):
    ff02::1
    ff02::2
    ff02::1:ff00:2
    ff02::1:ffa7:497e
  ND MTU is 0
  ICMP redirects are not sent
  DAD is enabled, number of DAD attempts: 3
  ND reachable time is 39610 milliseconds
  ND base reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 198 to 600 seconds
  ND router advertisements live for 1800 seconds
  ND advertised hop limit is 64
  IPv6 hop limit for originated packets is 64
Dell#
```

Example (Managementethernet)

```
Dell#show ipv6 int man 0/0
ManagementEthernet 0/0 is up, line protocol is up
  IPV6 is enabled
  Link Local address: fe80::201:e8ff:fea7:497e
  Global Unicast address(es):
   Actual address is 300::1, subnet is 300::/64 (MANUAL)
     Remaining lifetime: infinite
    Virtual-IP IPv6 address is not set
  Global Anycast address(es):
  Joined Group address(es):
    ff02::1
    ff02::1:ff00:1
    ff02::1:ffa7:497e
  ND MTU is 0
  ICMP redirects are not sent
  DAD is enabled, number of DAD attempts: 3
  ND reachable time is 20410 milliseconds
  ND base reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  ND hop limit is 64
Dell#
```

Example (Brief)

```
Dell#show ipv6 int brief
TenGigabitEthernet 0/2           [administratively down/down]
    fe80::201:e8ff:fea7:497e
    2002:1:2::3/96
TenGigabitEthernet 0/12          [up/up]
    fe80::201:e8ff:fea7:497e
    100::2/64
ManagementEthernet 0/0           [up/up]
    fe80::201:e8ff:fea7:497e
    300::1/64
Dell#
```

Example (tunnel)

```
Dell#show ipv6 int tun 1
Tunnel 1 is up, line protocol is up
  IPV6 is enabled
  Link Local address: fe80::201:e8ff:fea7:497e
  Global Unicast address(es):
    400::1, subnet is 400::/64 (MANUAL)
     Remaining lifetime: infinite
  Global Anycast address(es):
  Joined Group address(es):
    ff02::1
    ff02::2
    ff02::1:ff00:1
    ff02::1:ffa7:497e
  ND MTU is 0
  ICMP redirects are not sent
  DAD is enabled, number of DAD attempts: 3
  ND reachable time is 20410 milliseconds
  ND base reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 198 to 600 seconds
  ND router advertisements live for 1800 seconds
  ND advertised hop limit is 64
  IPv6 hop limit for originated packets is 64
Dell#
```

show ipv6 mld_host

Display the IPv6 MLD host counters.

Syntax `show ipv6 mld_host`

Command Modes EXEC

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information The following describes the `show ipv6 mld-host` command shown in the following example.

Field	Description
Valid MLD Packets	The total number of packets received and sent from the last time the elapsed time was cleared.
Reports	The total number of reports (queries and unsolicited reports generated from joins or leaves) that have been received or sent.
Leaves	The number of Multicast leaves that have been sent.
MLDv1 queries	The number of MLDv1 queries that have been received.

Field	Description
MLDv2 queries	The number of MLDv2 queries that have been received.
Malformed Packets	The number of MLDv1 and MLDv2 packets that do not match the requirement for a valid MLD packet.

Example

```
MLD Host Traffic Counters
Elapsed time since counters cleared: 0028:33:52
                     Received   Sent
Valid MLD Packets    97962      18036
Reports              79962      18034
Leaves               ----       0
MLDv2 Queries        18000      ----
MLDv1 Queries        0          ----
Errors:
Malformed Packets: 4510
```

show ipv6 route

Displays the IPv6 routes.

Syntax

```
show ipv6 route [ipv6-address prefix-length] [hostname] [all]
[bgp as number] [connected] [isis tag] [list prefix-list name]
[ospf process-id] [rip] [static] [summary]
```

Parameters

ipv6-address prefix-length	(OPTIONAL) Enter the IPv6 address in the x:x:x:x::x format then the prefix length in the /x format. The range is from /0 to /128. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
hostname	(OPTIONAL) View information for this IPv6 routes with Host Name.
all	(OPTIONAL) View information for all IPv6 routes.
bgp	(OPTIONAL) View information for all IPv6 BGP routes.
connected	(OPTIONAL) View only the directly connected IPv6 routes.
isis	(OPTIONAL) View information for all IPv6 IS-IS routes.
list	(OPTIONAL) View the IPv6 prefix list.
ospf	(OPTIONAL) View information for all IPv6 OSPF routes.
rip	(OPTIONAL) View information for all IPv6 RIP routes.
static	(OPTIONAL) View only routes configured by the `ipv6 route` command.
summary	(OPTIONAL) View a brief list of the configured IPv6 routes.

Defaults	none
Command Modes	• EXEC • EXEC Privilege
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show ipv6 route` command shown in the following examples.

Field	Description
(undefined)	Identifies the type of route: • L = Local • C = connected • S = static • R = RIP • B = BGP • IN = internal BGP • EX = external BGP • LO = Locally Originated • O = OSPF • IA = OSPF inter-area • N1 = OSPF NSSA external type 1 • N2 = OSPF NSSA external type 2 • E1 = OSPF external type 1 • E2 = OSPF external type 2 • i = IS-IS • L1 = IS-IS level-1 • L2 = IS-IS level-2 • IA = IS-IS inter-area • * = candidate default • > = non-active route • + = summary routes
Destination	Identifies the route's destination IPv6 address.
Gateway	Identifies whether the route is directly connected and on which interface the route is configured.
Dist/Metric	Identifies if the route has a specified distance or metric.
Last Change	Identifies when the route was last changed or configured.

Example

```
Dell#show ipv6 route

Codes: C - connected, L - local, S - static, R - RIP,
       B - BGP, IN - internal BGP, EX - external BGP,LO -
```

```
Locally Originated,
       O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external
type 1,
       N2 - OSPF NSSA external type 2, E1 - OSPF external type
1,
       E2 - OSPF external type 2, i - IS-IS, L1 - IS-IS
level-1,
       L2 - IS-IS level-2, IA - IS-IS inter area, * -
candidate default,
Gateway of last resort is not set

       Destination  Dist/Metric,      Gateway,   Last Change
       ----------------------------------------------------
  C    100::/64 [0/0]
          Direct, Te 0/12, 20:00:18
  C    400::/64 [0/0]
          Direct, Tu 1, 00:09:02
  S    800::/64 [1/0]
          via 100::1, Te 0/12, 00:00:50
  L    fe80::/10 [0/0]
          Direct, Nu 0, 20:00:18
Dell#
```

Example (Summary)

```
Dell#show ipv6 route summary
Route Source              Active Routes   Non-active Routes
connected                 3               0
static                    1               0
Total                     4               0
Total 4 active route(s) using 928 bytes
Dell#
```

trust ipv6-diffserv

Allows the dynamic classification of IPv6 DSCP.

Syntax

`trust ipv6-diffserv`

To remove the definition, use the `no trust ipv6-diffserv` command.

Defaults

none

Command Modes

CONFIGURATION-POLICY-MAP-IN

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

When you configure trust IPv6 diffserv, matched bytes/packets counters are not incremented in the `show qos statistics` command.

Trust diffserv (IPv4) can co-exist with trust ipv6-diffserv in an Input Policy Map. Dynamic classification happens based on the mapping as shown:

IPv6 Service Class Field	Queue ID
111XXXXX	7
110XXXXX	6
101XXXXX	5
100XXXXX	4
011XXXXX	3
010XXXXX	2
001XXXXX	1
000XXXXX	0

26

IPv6 Border Gateway Protocol (IPv6 BGP)

IPv6 Border Gateway Protocol (IPv6 BGP) is supported on Dell Networking platforms.

This chapter includes the following sections:

- IPv6 BGP Commands
- IPv6 MBGP Commands

IPv6 BGP Commands

BGP is an external gateway protocol that transmits interdomain routing information within and between autonomous systems (AS). BGP version 4 (BGPv4) supports classless interdomain routing and the aggregation of routes and AS paths. Basically, two routers (called neighbors or peers) exchange information including full routing tables and periodically send messages to update those routing tables.

The following commands allow you to configure and enable BGP.

address family

This command changes the context to subsequent address family identifier (SAFI).

Syntax	`address family ipv6 unicast` To remove SAFI context, use the `no address family ipv6 unicast` command.
Parameters	**ipv6** — Enter the keyword `ipv6` to specify the address family as IPv6. **unicast** — Enter the keyword `unicast` to specify multicast as SAFI.
Defaults	IPv6 Unicast
Command Modes	ROUTER BGPV6-ADDRESS FAMILY
Command History	Version 9.2(0.0) — Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

After this command is executed, all subsequent commands apply to this address family. You can exit from this AFI/SAFI to the IPv6 Unicast (the default) family by entering the `exit` command and returning to the Router BGP context.

aggregate-address

Summarize a range of prefixes to minimize the number of entries in the routing table.

Syntax

```
aggregate-address ipv6-address prefix-mength [advertise-map
map-name] [as-set] [attribute-map map-name] [summary-only]
[suppress-map map-name]
```

Parameters

ipv6-address prefix-length	Enter the IPv6 address in the x:x:x:x::x format then the prefix length in the / x format. The range is from /0 to /128. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
advertise-map *map-name*	(OPTIONAL) Enter the keywords `advertise-map` then the name of a configured route map to set filters for advertising an aggregate route.
as-set	(OPTIONAL) Enter the keywords `as-set` to generate path attribute information and include it in the aggregate. AS_SET includes AS_PATH and community information from the routes included in the aggregated route.
attribute-map *map-name*	(OPTIONAL) Enter the keywords `attribute-map` then the name of a configured route map to modify attributes of the aggregate, excluding AS_PATH and NEXT_HOP attributes.
summary-only	(OPTIONAL) Enter the keywords `summary-only` to advertise only the aggregate address. Specific routes are not advertised.
suppress-map *map-name*	(OPTIONAL) Enter the keywords `suppress-map` then the name of a configured route map to identify which more-specific routes in the aggregate are suppressed.

Defaults

Not configured.

Command Modes

- ROUTER BGP ADDRESS FAMILY
- ROUTER BGP ADDRESS FAMILY IPv6

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

At least one of the routes included in the aggregate address must be in the BGP routing table for the configured aggregate to become active.

Do not add the `as-set` parameter to the aggregate if routes within the aggregate are constantly changing as the aggregate will flap to keep track of the changes in the AS_PATH.

In route maps used in the `suppress-map` parameter, routes meeting the `deny` clause are not suppress; in other words, they are allowed. The opposite is true: routes meeting the `permit` clause are suppressed.

If the route is injected using the `network` command, that route still appears in the routing table if you configure the `summary-only` parameter in the `aggregate-address` command.

The `summary-only` parameter suppresses all advertisements. If you want to suppress advertisements to only specific neighbors, use the `neighbor distribute-list` command.

In the `show ip bgp ipv6 unicast` command, aggregates contain an ‘a’ in the first column and routes suppressed by the aggregate contain an ‘s’ in the first column.

bgp always-compare-med

Allows you to enable comparison of the MULTI_EXIT_DISC (MED) attributes in the paths from different external ASs.

Syntax

```
bgp always-compare-med
```

To disable comparison of MED, use the `no bgp always-compare-med` command.

Defaults

Disabled (that is, the software only compares MEDs from neighbors within the same AS).

Command Modes

ROUTER BGP

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Any update without a MED attribute is the least preferred route.

If you enable this command, use the `capture bgp-pdu max-buffer-size *` command to recompute the best path.

bgp bestpath as-path ignore

Ignore the AS PATH in BGP best path calculations.

Syntax	`bgp bestpath as-path ignore` To return to the default, use the `no bgp bestpath as-path ignore` command.
Defaults	Disabled (that is, the software considers the AS_PATH when choosing a route as best).
Command Modes	ROUTER BGP
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	If you enable this command, use the `capture bgp-pdu max-buffer-size *` command to recompute the best path.

bgp bestpath med confed

Enable MULTI_EXIT_DISC (MED) attribute comparison on paths learned from BGP confederations.

Syntax	`bgp bestpath med confed` To disable MED comparison on BGP confederation paths, use the `no bgp bestpath med confed` command.
Defaults	Disabled.
Command Modes	ROUTER BGP
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	The software compares the MEDs only if the path contains no external autonomous system numbers. If you enable this command, use the `capture bgp-pdu max-buffer-size *` command to recompute the best path.

bgp bestpath med missing-as-best

During path selection, indicate a preference to paths with missing MED (MULTI_EXIT_DISC) over those paths with an advertised MED attribute.

Syntax	`bgp bestpath med missing-as-best` To return to the default selection, use the `no bgp bestpath med missing-as-best` command.
Defaults	Disabled.
Command Modes	ROUTER BGP
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	The MED is a 4-byte unsigned integer value and the default behavior is to assume a missing MED as 4294967295. This command causes a missing MED to be treated as 0. During path selection, paths with a lower MED are preferred over those with a higher MED.

bgp client-to-client reflection

Allows you to enable route reflection between clients in a cluster.

Syntax	`bgp client-to-client reflection` To disable client-to-client reflection, use the `no bgp client-to-client reflection` command.
Defaults	Enabled when a route reflector is configured.
Command Modes	ROUTER BGP
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	Route reflection to clients is not necessary if all client routers are fully meshed.
Related Commands	bgp cluster-id — assigns and ID to a BGP cluster with two or more route reflectors. neighbor route-reflector-client — configures a route reflector and clients.

bgp cluster-id

Assign a cluster ID to a BGP cluster with more than one route reflector.

Syntax	`bgp cluster-id {ip-address	number}` To delete a cluster ID, use the `no bgp cluster-id {ip-address	number}` command.
Parameters	*ip-address* — Enter an IP address as the route reflector cluster ID. *number* — Enter a route reflector cluster ID as a number from 1 to 4294967295.
Defaults	Not configured.
Command Modes	ROUTER BGP
Command History	Version 9.2(0.0) — Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	When a BGP cluster contains only one route reflector, the cluster ID is the route reflector's router ID. For redundancy, a BGP cluster may contain two or more route reflectors and you assign a cluster ID with the `bgp cluster-id` command. Without a cluster ID, the route reflector cannot recognize route updates from the other route reflectors within the cluster. The default format for displaying the cluster-id is dotted decimal, but if you enter the cluster-id as an integer, it displays as an integer.
Related Commands	bgp client-to-client reflection — enables route reflection between the route reflector and the clients. neighbor route-reflector-client — configures a route reflector and clients. show ip bgp ipv6 unicast cluster-list — views paths with a cluster ID.

bgp confederation identifier

Configure an identifier for a BGP confederation.

Syntax	`bgp confederation identifier as-number` To delete a BGP confederation identifier, use the `no bgp confederation identifier as-number` command.
Parameters	*as-number* — Enter the AS number. The range is from 1 to 65535.

Defaults	Not configured.
Command Modes	ROUTER BGP
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	The autonomous systems configured in this command are visible to the EBGP neighbors. Each autonomous system is fully meshed and contains a few connections to other autonomous systems. The next hop, MED, and local preference information is preserved throughout the confederation. The system accepts confederation EBGP peers without a LOCAL_PREF attribute. The software sends AS_CONFED_SET and accepts AS_CONFED_SET and AS_CONF_SEQ.

bgp confederation peers

Specify the autonomous systems (ASs) that belong to the BGP confederation.

Syntax

```
bgp confederation peers as-number [...as-number]
```

To remove bgp confederation peers, use the `no bgp confederation peer` command.

Parameters

as-number	Enter the AS number. The range is 1 to 65535.
...as-number	(OPTIONAL) Enter up to 16 confederation numbers. The range is from 1 to 65535.

Defaults	Not configured.
Command Modes	ROUTER BGP
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	The Autonomous Systems configured in this command are visible to the EBGP neighbors. Each Autonomous System is fully meshed and contains a few connections to other Autonomous Systems. After specifying autonomous systems numbers for the BGP confederation, recycle the peers to update their configuration.
Related Commands	bgp confederation identifier — configures a confederation ID.

bgp dampening

Enable BGP route dampening and configure the dampening parameters.

Syntax

```
bgp dampening [half-life reuse suppress max-suppress-time]
[route-map map-name]
```

Parameters

half-life	(OPTIONAL) Enter the number of minutes after which the Penalty is decreased. After the router assigns a Penalty of 1024 to a route, the Penalty is decreased by half, after the half-life period expires. The range is from 1 to 45. The default is **15 minutes**.
reuse	(OPTIONAL) Enter a number as the reuse value, which is compared to the flapping route's Penalty value. If the Penalty value is less than the reuse value, the flapping route is once again advertised (or no longer suppressed). The range is from 1 to 20000. The default is **750**.
suppress	(OPTIONAL) Enter a number as the suppress value, which is compared to the flapping route's Penalty value. If the Penalty value is greater than the suppress value, the flapping route is no longer advertised (that is, it is suppressed). The range is from 1 to 20000. The default is **2000**.
max-suppress-time	(OPTIONAL) Enter the maximum number of minutes a route can be suppressed. The default is four times the half-life value. The range is from 1 to 255. The default is **60 minutes**.
route-map *map-name*	(OPTIONAL) Enter the keywords `route-map` then the name of a configured route map. Only match commands in the configured route map are supported.

Defaults Disabled.

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information If you enter `bgp dampening`, the default values for `half-life`, `reuse`, `suppress`, and `max-suppress-time` are applied. The parameters are position-dependent; therefore, if you configure one parameter, you must configure the parameters in the order they appear in the command.

Related Commands show ip bgp ipv6 unicast dampened-paths — views the BGP paths.

bgp default local-preference

Change the default local preference value for routes exchanged between internal BGP peers.

Syntax	`bgp default local-preference value` To return to the default value, use the `no bgp default local-preference` command.
Parameters	**value**: Enter a number to assign to routes as the degree of preference for those routes. When routes are compared, the higher the degree of preference or local preference value, the more the route is preferred. The range is from 0 to 4294967295. The default is **100**.
Defaults	**100**
Command Modes	ROUTER BGP
Command History	Version 9.2(0.0): Introduced on the MXL 10/40GbE Switch IO Module.

bgp enforce-first-as

Disable (or enable) enforce-first-as check for updates received from EBGP peers.

Syntax	`bgp enforce-first-as` To turn off the default, use the `no bgp enforce-first-as` command.
Defaults	Enabled.
Command Modes	ROUTER BGP
Command History	Version 9.2(0.0): Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	This is enabled by default; that is, for all updates received from EBGP peers, BGP ensures that the first AS of the first AS segment is always the AS of the peer. If not, the update is dropped and a counter is incremented. To view the failed enforce-first-as check counter, use the `show ip bgp ipv6 unicast neighbors` command. If you disable `enforce-first-as`, view it using the `show ip protocols` command.

Related Commands	show ip bgp ipv6 unicast neighbors — displays IPv6 routing information exchanged by BGP neighbors. show ip protocols — views information on routing protocols.

bgp fast-external-fallover

Enable the fast external fallover feature, which immediately resets the BGP session if a link to a directly connected external peer fails.

Syntax	`bgp fast-external-fallover` To disable fast external fallover, use the `no bgp fast-external-fallover` command.
Defaults	Enabled.
Command Modes	ROUTER BGP
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	The `bgp fast-external-fallover` command appears in the `show config` command output.

bgp four-octet-as-support

Enable 4-byte support for the BGP process.

Syntax	`bgp four-octet-as-support` To disable fast external fallover, use the `no bgp four-octet-as-support` command.
Defaults	Disabled (supports 2-Byte format)
Command Modes	ROUTER BGP
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	Routers supporting 4-Byte ASNs advertise that function in the OPEN message. The behavior of a 4-Byte router is slightly different depending on whether it is speaking to a 2-Byte router or a 4-Byte router.

When creating Confederations, all the routers in the Confederation must be 4- or 2-byte identified routers. You cannot mix them.

Where the 2-Byte format is from 1 to 65535, the 4-Byte format is from 1 to 4294967295. Both formats are accepted, and the advertisements reflect the entered format.

For more information about using the 2- or 4-Byte format, refer to the *Dell Networking OS Configuration Guide*.

bgp graceful-restart

Enable graceful restart on a BGP neighbor, a BGP node, or designate a local router to support graceful restart as a receiver only.

Syntax

`bgp graceful-restart [restart-time seconds] [stale-path-time seconds] [role receiver-only]`

To return to the default, enter the `no bgp graceful-restart` command.

Parameters

neighbor *ip-address* | *peer-group-name*	Enter the keyword `neighbor` then one of the options: • *`ip-address`* of the neighbor in IP address format of the neighbor • *`peer-group-name`* of the neighbor peer group
restart-time *seconds*	Enter the keywords `restart-time` then the maximum number of seconds needed to restart and bring up all peers. The range is from 1 to 3600 seconds. The default is **120 seconds**.
stale-path-time *seconds*	Enter the keywords `stale-path-time` then the maximum number of seconds to wait before restarting a peer's stale paths. The default is **360 seconds**.
role *receiver-only*	Enter the keywords `role receiver-only` to designate the local router to support graceful restart as a receiver only.

Defaults

As above

Command Modes

ROUTER BGP

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

This feature is advertised to BGP neighbors through a capability advertisement. In Receiver Only mode, BGP saves the advertised routes of peers that support this capability when they restart.

bgp log-neighbor-changes

Enable logging of BGP neighbor resets.

Syntax

```
bgp log-neighbor-changes
```

To disable logging, use the `no bgp log-neighbor-changes` command.

Defaults

Enabled.

Command Modes

ROUTER BGP

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The `bgp log-neighbor-changes` command appears in the `show config` command output.

Related Commands

show config — views the current configuration.

bgp non-deterministic-med

Compare MEDs of paths from different autonomous systems (ASs).

Syntax

```
bgp non-deterministic-med
```

To return to the default, use the `no bgp non-deterministic-med` command.

Defaults

Disabled (that is, paths/routes for the same destination but from different ASs does not have their MEDs compared).

Command Modes

ROUTER BGP

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

In Non-Deterministic mode, paths are compared in the order in which they arrive. This method can lead to the system choosing different best paths from a set of paths, depending on the order in which they are received from the neighbors because MED may or may not get compared between adjacent paths. In Deterministic mode (`no bgp non-deterministic-med`), the system compares MED between adjacent paths within an AS group because all paths in the AS group are from the same AS.

When you change the path selection from Deterministic to Non-Deterministic mode, the path selection for existing paths remains Deterministic until you enter the `capture bgp-pdu max-buffer-size` command to clear existing paths.

bgp recursive-bgp-next-hop

Enable next-hop resolution through other routes learned by BGP.

Syntax

`bgp recursive-bgp-next-hop`

To disable next-hop resolution, use the `no bgp recursive-bgp-next-hop` command.

Defaults

Enabled.

Command Modes

ROUTER BGP

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

This command is a knob to disable BGP next-hop resolution using BGP learned routes. During the next-hop resolution, only the first route that the next-hop resolves through is verified for the route's protocol source and is checked if the route is learned from BGP or not.

For this command to take effect and to keep the BGP database consistent, you need the `clear ip bgp` command. Execute the `clear ip bgp` command right after executing this command.

Related Commands

capture bgp-pdu max-buffer-size

bgp regex-eval-optz-disable

Disables the Regex Performance engine that optimizes complex regular expression with BGP.

Syntax

`bgp regex-eval-optz-disable`

To re-enable optimization engine, use the `no bgp regex-eval-optz-disable` command.

Defaults

Enabled.

Command Modes

ROUTER BGP (conf-router_bgp)

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

BGP uses regular expressions (regex) to filter route information. In particular, the use of regular expressions to filter routes based on AS-PATHs and communities is quite common. In a large scale configuration, filtering millions of routes based on regular expressions can be quite CPU intensive, as a regular expression evaluation involves generation and evaluation of complex finite state machines.

BGP policies, containing regular expressions to match as-path and communities, tend to use a lot of CPU processing time, which in turn affects the BGP routing convergence. Additionally, the `show bgp` commands, which are filtered through regular expressions, use up CPU cycles particularly with large databases. The Regex Engine Performance Enhancement feature optimizes the CPU usage by caching and reusing regular expression evaluation results. This caching and reuse may be at the expensive of RP1 processor memory.

Related Commands

show ip protocols — views information on all routing protocols enabled and active.

bgp router-id

Assign a user-given ID to a BGP router.

Syntax

`bgp router-id ip-address`

To delete a user-assigned IP address, use the `no bgp router-id` command.

Parameters

ip-address	Enter an IP address in dotted decimal format to reset only that BGP neighbor.

Defaults

The router ID is the highest IP address of the Loopback interface or, if no Loopback interfaces are configured, the highest IP address of a physical interface on the router.

Command Modes

ROUTER BGP

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Peering sessions are reset when you change the router ID of a BGP router.

bgp soft-reconfig-backup

Use this command *only* when route-refresh is *not* negotiated between peers to avoid having a peer re-send BGP updates.

Syntax

`bgp soft-reconfig-backup`

To return to the default setting, use the `no bgp soft-reconfig-backup` command.

Defaults

Off

Command Modes	ROUTER BGPV6 ADDRESS FAMILY (conf-router_bgpv6_af)
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	When you enable soft-reconfiguration for a neighbor and you execute the `clear ip bgp soft in` command, the update database stored in the router replays and updates are reevaluated. With this command, the replay and update process is triggered only if route-refresh request is *not* negotiated with the peer. If the request is negotiated (after execution of `clear ip bgp soft in`), BGP sends a route-refresh request to the neighbor and receives all of the peer's updates.
Related Commands	clear ip bgp ipv6 unicast soft — activates inbound policies for IPv6 routes without resetting the BGP TCP session.

capture bgp-pdu neighbor (ipv6)

Enable capture of an IPv6 BGP neighbor packet.

Syntax

```
capture bgp-pdu neighbor ipv6-address direction {both | rx |
tx}
```

To disable capture of the IPv6 BGP neighbor packet, use the `no capture bgp-pdu neighbor ipv6-address` command.

Parameters

ipv6-address	Enter the IPv6 address of the target BGP neighbor.
direction {both | rx | tx}	Enter the keyword `direction` and a direction — either `rx` for inbound, `tx` for outbound, or both.

Defaults: Not configured.

Command Modes

- EXEC
- EXEC Privilege

Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

capture bgp-pdu max-buffer-size — enables route reflection between the route reflector and the clients.

show capture bgp-pdu neighbor — configures a route reflector and clients.

capture bgp-pdu max-buffer-size

Set the size of the BGP packet capture buffer. This buffer size pertains to both IPv4 and IPv6 addresses.

Syntax

```
capture bgp-pdu max-buffer-size 100-102400000
```

Parameters

100-102400000	Enter a size for the capture buffer.

Defaults

40960000 bytes

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

capture bgp-pdu neighbor (ipv6) — enables route reflection between the route reflector and the clients.

show capture bgp-pdu neighbor — configures a route reflector and clients.

clear ip bgp * (asterisk)

Reset all BGP sessions in the specified category. The soft parameter (BGP Soft Reconfiguration) clears the policies without resetting the TCP connection.

Syntax

```
clear ip bgp * [ipv4 multicast soft [in | out] | ipv6 unicast
soft [in | out] | soft [in | out]]
```

Parameters

*	Enter an asterisk (`*`) to reset all BGP sessions.
ipv4 multicast soft [in | out]	(OPTIONAL) Enter the keywords `ipv4 multicast soft [in	out]` to set options within the specified IPv4 address family.
ipv6 unicast soft [in | out]	(OPTIONAL) Enter the keywords `ipv6 multicast soft [in	out]` to set options within the specified IPv6 address family.
soft	(OPTIONAL) Enter the keyword `soft` to configure and activate policies without resetting the BGP TCP session, that is, BGP Soft Reconfiguration. NOTE: If you enter `clear ip bgp ip6-address soft`, both inbound and outbound policies are reset.
in	(OPTIONAL) Enter the keyword `in` to activate only inbound policies.

out	(OPTIONAL) Enter the keyword `out` to activate only outbound policies.

Command Modes EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

clear ip bgp as-number

Reset BGP sessions. The soft parameter (BGP Soft Reconfiguration) clears the policies without resetting the TCP connection.

Syntax

```
clear ip bgp as-number [flap-statistics | ipv4 {multicast
{flap-statistics | soft {in | out}} | unicast {flap-statistics
| soft {in | out}} | ipv6 unicast {flap-statistics | soft {in |
out}| soft [in | out]
```

Parameters

as-number	Enter an autonomous system (AS) number to reset neighbors belonging to that AS. If used without a qualifier, the keyword resets all neighbors belonging to that AS. The range is from 1 to 65535.
flap-statistics	(OPTIONAL) Enter the keywords `flap-statistics` to clear all flap statistics belonging to that AS or a specified address family within that AS.
ipv4	(OPTIONAL) Enter the keyword `ipv4` to select options for that address family.
ipv6	(OPTIONAL) Enter the keyword `ipv6` to select options for that address family.
unicast	(OPTIONAL) Enter the keyword `unicast` to select the unicast option within the selected address family.
multicast	(OPTIONAL) Enter the keyword `multicast` to select the multicast option within the selected address family. Multicast is supported on IPv4 only.
soft	(OPTIONAL) Enter the keyword `soft` to configure and activate policies without resetting the BGP TCP session; that is, BGP Soft Reconfiguration. **NOTE:** If you enter `clear ip bgp ipv6-address soft`, both inbound and outbound policies are reset.
in	(OPTIONAL) Enter the keyword `in` to activate only inbound policies.

out	(OPTIONAL) Enter the keyword `out` to activate only outbound policies.

Command Modes EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

clear ip bgp ipv6-address

Reset BGP sessions specific to an IPv6 address. The soft parameter (BGP Soft Reconfiguration) clears the policies without resetting the TCP connection.

Syntax

```
clear ip bgp ipv6-address [flap-statistics | ipv4 {multicast
{flap-statistics | soft {in | out}} | unicast {flap-statistics
| soft {in | out}} | ipv6 unicast {flap-statistics | soft {in |
out}| soft [in | out]
```

Parameters

ipv6-address	Enter an IPv6 address to reset neighbors belonging to that IP. Used without a qualifier, the keyword `ipv6-address` resets all neighbors belonging to that IP.
flap-statistics	(OPTIONAL) Enter the keywords `flap-statistics` to clear all flap statistics belonging to that AS or a specified address family within that IP.
ipv4	(OPTIONAL) Enter the keyword `ipv4` to select options for that address family.
ipv6	(OPTIONAL) Enter the keyword `ipv6` to select options for that address family.
unicast	(OPTIONAL) Enter the keyword `unicast` to select the unicast option within the selected address family.
multicast	(OPTIONAL) Enter the keyword `multicast` to select the multicast option within the selected address family. Multicast is supported on IPv4 only.
soft	(OPTIONAL) Enter the keyword `soft` to configure and activate policies without resetting the BGP TCP session; that is, BGP Soft Reconfiguration. **NOTE:** If you enter `clear ip bgp ip6-address soft`, both inbound and outbound policies are reset.
in	(OPTIONAL) Enter the keyword `in` to activate only inbound policies.
out	(OPTIONAL) Enter the keyword `out` to activate only outbound policies.

Command Modes	EXEC Privilege
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.

clear ip bgp peer-group

Reset a peer-group's BGP sessions.

Syntax

```
clear ip bgp peer-group peer-group-name
```

Parameters

peer-group-name	Enter the peer group name to reset the BGP sessions within that peer group.

Command Modes	EXEC Privilege
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.

clear ip bgp ipv6 dampening

Clear information on route dampening and return suppressed route to active state.

Syntax

```
clear ip bgp ipv6 unicast dampening [ipv6-address]
```

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format then the prefix length in the /x format. The range is from /0 to /128. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.

Command Modes	EXEC Privilege
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	After you enter this command, the software deletes the history routes and returns the suppressed routes to the active state.

clear ip bgp ipv6 flap-statistics

Clear BGP flap statistics, which includes number of flaps and the time of the last flap.

Syntax

```
clear ip bgp ipv6 unicast flap-statistics [ipv6-address |
filter-list as-path-name | regexp regular-expression]
```

Parameters

ipv6-address	(OPTIONAL) Enter the IPv6 address in the x:x:x:x::x format then the prefix length in the /x format. The range is from /0 to /128. NOTE: The :: notation specifies successive hexadecimal fields of zeros.
filter-list *as-path-name*	(OPTIONAL) Enter the keywords `filter-list` then the name of a configured AS-PATH list.
regexp *regular-expression*	(OPTIONAL) Enter the keyword `regexp` then the regular expressions. Use one or a combination of the following: • . (period) matches on any single character, including white space • * (asterisk) matches on sequences in a pattern (zero or more sequences) • + (plus sign) matches on sequences in a pattern (one or more sequences) • ? (question mark) matches sequences in a pattern (0 or 1 sequences) • [ ] (brackets) matches a range of single-character patterns. • ^ (caret) matches the beginning of the input string. (If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified.) • $ (dollar sign) matches the end of the output string.

Command Modes

EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

If you enter the `clear ip bgp ipv6 flap-statistics` command without parameters, all the statistics clear.

Related Commands

show ip bgp ipv6 unicast flap-statistics — views BGP flap statistics.

clear ip bgp ipv6 unicast soft

Clear and reapply policies for IPv6 unicast routes without resetting the TCP connection; that is, perform BGP soft reconfiguration.

Syntax

```
clear ip bgp {* | as-number | ipv4-neighbor-addr | ipv6-
neighbor-addr | peer-group name} ipv6 unicast soft [in | out]
```

Parameters

*	Clear and reapply policies for all BGP sessions.
as-number	Clear and reapply policies for all neighbors belonging to the AS. The range is from 0 to 65535 (2 Byte), from 1 to 4294967295 (4 Byte), or from 0.1 to 0.65535.65535 (Dotted format).
ipv4-neighbor-addr | ipv6-neighbor-addr	Clear and reapply policies for a neighbor.
peer-group *name*	Clear and reapply policies for all BGP routers in the specified peer group.
ipv6 unicast	Clear and reapply policies for all IPv6 unicast routes.
in	Reapply only inbound policies. **NOTE:** If you enter `soft`, without an `in` or `out` option, both inbound and outbound policies are reset.
out	Reapply only outbound policies. **NOTE:** If you enter `soft`, without an `in` or `out` option, both inbound and outbound policies are reset.

Command Modes EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

debug ip bgp

Allows you to view all information on BGP, including BGP events, keepalives, notifications, and updates.

Syntax

```
debug ip bgp [ipv6-address | peer-group peer-group-name] [in |
out]
```

To disable all BGP debugging, use the `no debug ip bgp` command.

Parameters

ipv6-address	(OPTIONAL) Enter the IPv6 address in the x:x:x:x::x format then the prefix length in the /x format. The range is from /0 to /128.

NOTE: The :: notation specifies successive hexadecimal fields of zeros.

peer-group *peer-group-name*	Enter the keywords `peer-group` then the name of the peer group.
in	(OPTIONAL) Enter the keyword `in` to view only information on inbound BGP routes.
out	(OPTIONAL) Enter the keyword `out` to view only information on outbound BGP routes.

Command Modes

EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To view information on both incoming and outgoing routes, do not include the `in` and `out` parameters in the `debugging` command. The `in` and `out` parameters cancel each other; for example, if you enter `debug ip bgp in` and then enter `debug ip bgp out`, you do not see information on the incoming routes.

Entering a `no debug ip bgp` command removes all configured debug commands for BGP.

Related Commands

debug ip bgp events — views information about BGP events.

debug ip bgp keepalives — views information about BGP keepalives.

debug ip bgp notifications — views information about BGP notifications.

debug ip bgp updates — views information about BGP updates.

debug ip bgp events

Allows you to view information on local BGP state changes and other BGP events.

Syntax

```
debug ip bgp [ipv6-address | peer-group peer-group-name] events
[in | out]
```

To disable debugging, use the `no debug ip bgp ipv6-address | peer-group peer-group-name] events` command.

Parameters

ipv6-address	(OPTIONAL) Enter the IPv6 address in the x:x:x:x::x format then the prefix length in the /x format. The range is from /0 to /128.

NOTE: The :: notation specifies successive hexadecimal fields of zeros.

peer-group *peer-group-name*	Enter the keywords `peer-group` then the name of the peer group.
in	(OPTIONAL) Enter the keyword `in` to view only information on inbound BGP routes.
out	(OPTIONAL) Enter the keyword `out` to view only information on outbound BGP routes.

Command Modes

EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Entering a `no debug ip bgp` command removes all configured debug commands for BGP.

debug ip bgp ipv6 dampening

View information on dampened (non-active) IPv6 routes.

Syntax

```
debug ip bgp ipv6 unicast dampening [in | out]
```

To disable debugging, use the `no debug ip bgp ipv6 unicast dampening` command.

Parameters

in	(OPTIONAL) Enter the keyword `in` to view only inbound dampened routes.
out	(OPTIONAL) Enter the keyword `out` to view only outbound dampened routes.

Command Modes

EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Entering a `no debug ip bgp` command removes all configured debug commands for BGP.

Related Commands

show ip bgp ipv6 unicast dampened-paths — views BGP dampened routes.

debug ip bgp ipv6 unicast soft-reconfiguration

Enable soft-reconfiguration debugging for IPv6 unicast routes.

Syntax

```
debug ip bgp [ipv4-address | ipv6-address | peer-group-name]
ipv6 unicast soft-reconfiguration
```

To disable debugging, use the `no debug ip bgp [ipv4-address | ipv6-address | peer-group-name] ipv6 unicast soft-reconfiguration` command.

Parameters

ipv4-address | *ipv6-address*	Enter the IP address of the neighbor on which you want to enable soft-reconfiguration debugging.
peer-group-name	Enter the name of the peer group on which you want to enable soft-reconfiguration debugging.
ipv6 unicast	Debug soft reconfiguration for IPv6 unicast routes.

Defaults

Disabled.

Command Modes

EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

This command turns on BGP soft-reconfiguration inbound debugging for IPv6 unicast routes. If no neighbor is specified, debug is turned on for all neighbors.

Related Commands

show ip bgp ipv6 unicast dampened-paths — views BGP dampened routes.

debug ip bgp keepalives

Allows you to view information about BGP keepalive messages.

Syntax

```
debug ip bgp [ipv6-address | peer-group peer-group-name]
keepalives [in | out]
```

To disable debugging, use the `no debug ip bgp [ip-address | peer-group peer-group-name] keepalives [in | out]` command.

Parameters

ipv6-address	(OPTIONAL) Enter the IPv6 address in the x:x:x:x::x format then the prefix length in the /x format. The range is /0 to /128. NOTE: The :: notation specifies successive hexadecimal fields of zeros.

peer-group *peer-group-name*	(OPTIONAL) Enter the keywords `peer-group` then the name of the peer group.
in	(OPTIONAL) Enter the keyword `in` to view only inbound keepalive messages.
out	(OPTIONAL) Enter the keyword `out` to view only outbound keepalive messages.

Command Modes

EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Entering a `no debug ip bgp` command removes all configured debug commands for BGP.

debug ip bgp notifications

Allows you to view information about BGP notifications received from neighbors.

Syntax

```
debug ip bgp [ipv6-address | peer-group peer-group-name]
notifications [in | out]
```

To disable debugging, use the `no debug ip bgp [ip-address | peer-group peer-group-name] notifications [in | out]` command.

Parameters

ipv6-address	(OPTIONAL) Enter the IPv6 address in the x:x:x:x::x format then the prefix length in the /x format. The range is from /0 to /128. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
peer-group *peer-group-name*	(OPTIONAL) Enter the keywords `peer-group` then the name of the peer group.
in	(OPTIONAL) Enter the keyword `in` to view BGP notifications received from neighbors.
out	(OPTIONAL) Enter the keyword `out` to view BGP notifications sent to neighbors.

Command Modes

EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Entering a `no debug ip bgp` command removes all configured debug commands for BGP.

debug ip bgp updates

Allows you to view information about BGP updates.

Syntax

```
debug ip bgp [ipv6-address | peer-group peer-group-name | ipv6
unicast [ipv6-address]] updates [in | out | prefix-list prefix-
list-name]
```

To disable debugging, use the `no debug ip bgp [ip-address | peer-group peer-group-name | ipv6 unicast [ipv6-address]] updates [in | out]` command.

Parameters

ipv6-address	(OPTIONAL) Enter the IPv6 address in the x:x:x:x::x format then the prefix length in the /x format. The range is from /0 to /128. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
peer-group *peer-group-name*	(OPTIONAL) Enter the keywords `peer-group` then the name of the peer group.
ipv6 unicast [*ipv6-address*]	(OPTIONAL) Enter the keywords `ipv6 unicast`, and, optionally, an ipv6 address.
in	(OPTIONAL) Enter the keyword `in` to view only BGP updates received from neighbors.
out	(OPTIONAL) Enter the keyword `out` to view only BGP updates sent to neighbors.

Command Modes

EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Entering a `no debug ip bgp` command removes all configured debug commands for BGP.

default-metric

Allows you to change the metrics of redistributed routes to locally originated routes. Use this command with the `redistribute` command.

Syntax

`default-metric` *`number`*

To return to the default setting, use the `no default-metric` command.

Parameters

number	Enter a number as the metric to be assigned to routes from other protocols. The range is from 1 to 4294967295.

Defaults

0

Command Modes

ROUTER BGP

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The `default-metric` command in BGP sets the value of the BGP MULTI_EXIT_DISC (MED) attribute for redistributed routes only.

Related Commands

bgp always-compare-med — enables comparison of all BGP MED attributes.

redistribute — redistributes routes from other routing protocols into BGP.

description

Enter a description of the BGP routing protocol.

Syntax

`description {`*`description`*`}`

To remove the description, use the no description {*description*} command.

Parameters

description	Enter a description to identify the BGP protocol (80 characters maximum).

Defaults

none

Command Modes

ROUTER BGP

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

router bgp — enters ROUTER mode on the switch.

distance bgp

Configure three administrative distances for routes.

Syntax `distance bgp external-distance internal-distance local-distance`

To return to default values, use the `no distance bgp` command.

Parameters

external-distance	Enter a number to assign to routes learned from a neighbor external to the AS. The range is from 1 to 255. The default is **20**.
internal-distance	Enter a number to assign to routes learned from a router within the AS. The range is from 1 to 255. The default is **200**.
local-distance	Enter a number to assign to routes learned from networks listed in the network command. The range is from 1 to 255. The default is **200**.

Defaults

- external-distance = **20**
- internal-distance = **200**
- local-distance = **200**

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

CAUTION: Dell Force10 recommends that you do not change the administrative distance of internal routes. Changing the administrative distances may cause routing table inconsistencies.

The higher the administrative distance assigned to a route means that your confidence in that route is low. Routes assigned an administrative distance of 255 are not installed in the routing table.

Routes from confederations are treated as internal BGP routes.

maximum-paths

Configure the maximum number of parallel routes (multipath support) BGP supports.

Syntax `maximum-paths {ebgp | ibgp} number`

To return to the default values, use the `no maximum-paths` command.

Parameters

ebgp	Enter the keyword `ebgp` to enable multipath support for External BGP routes.
ibgp	Enter the keyword `ibgp` to enable multipath support for Internal BGP routes.
number	Enter a number as the maximum number of parallel paths. The range is from 1 to 16. The default is **1**.

Defaults **1**

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information If you enable this command, use the `capture bgp-pdu max-buffer-size` command to recompute the best path.

neighbor activate

This command allows the specified neighbor/peer group to be enabled for the current AFI/SAFI.

Syntax `neighbor {ipv6-address | peer-group-name} activate`

To disable, use the `no neighbor {ipv6-address | peer-group-name} activate` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. NOTE: The :: notation specifies successive hexadecimal fields of zeros.
peer-group-name	Identify a peer group by name.
activate	Enter the keyword `activate` to enable the identified neighbor or peer group in the new AFI/SAFI.

Defaults Disabled.

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

By default, when you create a neighbor/peer group configuration in the Router BGP context, it is enabled for the IPv6/Unicast AFI/SAFI. By using `activate` in the new context, the neighbor/peer group is enabled for AFI/SAFI.

neighbor advertisement-interval

Set the advertisement interval between BGP neighbors or within a BGP peer group.

Syntax

```
neighbor {ipv6-address | peer-group-name} advertisement-interval seconds
```

To return to the default value, use the `no neighbor {ipv6-address | peer-group-name} advertisement-interval` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. NOTE: The :: notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group to set the advertisement interval for all routers in the peer group.
seconds	Enter a number as the time interval, in seconds, between BGP advertisements. The range is from 0 to 600 seconds. The default is **5 seconds** for internal BGP peers and **30 seconds** for external BGP peers.

Defaults

- seconds = **5 seconds** (internal peers)
- seconds = **30 seconds** (external peers)

Command Modes

ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

neighbor allowas-in

Set the number of times an AS number can occur in the AS path.

Syntax

```
neighbor {ip-address | peer-group-name} allowas-in number
```

To return to the default value, use the `no neighbor {ip-address | peer-group-name} allowas-in` command.

Parameters

ip-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group to set the advertisement interval for all routers in the peer group.
number	Enter a number of times to allow this neighbor ID to use the AS path. The range is from 1 to 10.

Defaults Not configured.

Command Modes ROUTER BGP

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands bgp four-octet-as-support — enables 4-Byte support for the BGP process.

neighbor default-originate

Inject the default route to a BGP peer or neighbor.

Syntax

```
neighbor {ipv6-address | peer-group-name} default-originate
[route-map map-name]
```

To remove a default route, use the `no neighbor {ipv6-address | peer-group-name} default-originate [route-map map-name]` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group to set the default route of all routers in that peer group.
route-map *map-name*	(OPTIONAL) Enter the keywords `route-map` then the name of a configured route map.

Defaults Not configured.

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

If you apply a route map to a BGP peer or neighbor with the `neighbor default-originate` command configured, the software does not apply the set filters in the route map to that BGP peer or neighbor.

neighbor description

Assign a character string describing the neighbor or group of neighbors (peer group).

Syntax

```
neighbor {ipv6-address | peer-group-name} description text
```

To delete a description, use the `no neighbor {ipv6-address | peer-group-name} description text` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. NOTE: The :: notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group.
text	Enter a continuous text string up to 80 characters.

Defaults

Not configured.

Command Modes

ROUTER BGP

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

neighbor distribute-list

Distribute BGP information using an established prefix list.

Syntax

```
neighbor {ipv6-address | peer-group-name} distribute-list
prefix-list-name {in | out}
```

To delete a neighbor distribution list, use the `no neighbor {ipv6-address | peer-group-name} distribute-list prefix-list-name {in | out}` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. NOTE: The :: notation specifies successive hexadecimal fields of zeros.

peer-group-name	Enter the name of the peer group.
prefix-list-name	Enter the name of an established prefix list. If the prefix list is not configured, the default is **permit** (to allow all routes).
in	Enter the keyword in to distribute only inbound traffic.
out	Enter the keyword out to distribute only outbound traffic.

Defaults

Not configured.

Command Modes

ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

neighbor filter-list — assigns a AS-PATH list to a neighbor or peer group.

neighbor route-map — assigns a route map to a neighbor or peer group.

neighbor ebgp-multihop

Attempt and accept BGP connections to external peers on networks that are not directly connected.

Syntax

`neighbor {ipv6-address | peer-group-name} ebgp-multihop [ttl]`

To disallow and disconnect connections, use the `no neighbor {ipv6-address | peer-group-name} ebgp-multihop [ttl]` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. NOTE: The :: notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group.
ttl	(OPTIONAL) Enter the number of hops as the time to live (ttl) value. The range is from 1 to 255. The default is **255**.

Defaults

Disabled.

Command Modes

ROUTER BGP

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information	To prevent loops, the `neighbor ebgp-multihop` command does not install default routes of the multihop peer. Networks not directly connected are not considered valid for best path selection.

neighbor fall-over

Enable or disable fast fall-over for BGP neighbors.

Syntax

`neighbor {ipv6-address | peer-group-name} fall-over`

To disable, use the `no neighbor {ipv6-address | peer-group-name} fall-over` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group.

Defaults	Disabled.
Command Modes	ROUTER BGP
Command History	Version 9.2(0.0) — Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	When you enable fall-over, BGP keeps track of IP or IPv6 reachability to the peer remote address and the peer local address. Whenever either address becomes unreachable (for examle, no active route exists in the routing table for peer IP or IPv6 destination/local address), BGP brings down the session with the peer.
Related Commands	show ip bgp ipv6 unicast neighbors — displays IPv6 routing information exchanged by BGP neighbors.

neighbor filter-list

Configure a BGP filter based on the AS-PATH attribute.

Syntax

`neighbor {ipv6-address | peer-group-name} filter-list as-path-name {in | out}`

To delete a BGP filter, use the `no neighbor {ipv6-address | peer-group-name} filter-list as-path-name {in | out}` command.

Parameters	*ipv6-address*	Enter the IPv6 address in the x:x:x:x::x format. NOTE: The :: notation specifies successive hexadecimal fields of zeros.
	peer-group-name	Enter the name of the peer group to apply the filter to all routers in the peer group.
	in	Enter the keyword `in` to filter inbound BGP routes.
	out	Enter the keyword `out` to filter outbound BGP routes.

Defaults: Not configured.

Command Modes: ROUTER BGPV6-ADDRESS FAMILY

Command History	Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

neighbor maximum-prefix

Control the number of network prefixes received.

Syntax

```
neighbor {ipv6-address | peer-group-name} maximum-prefix
maximum [threshold] [warning-only]
```

To return to the default values, use the `no neighbor {ipv6-address | peer-group-name} maximum-prefix maximum [threshold] [warning-only]` command.

Parameters	*ipv6-address*	Enter the IPv6 address in the x:x:x:x::x format. NOTE: The :: notation specifies successive hexadecimal fields of zeros.
	peer-group-name	Enter the name of the peer group.
	maximum	Enter a number as the maximum number of prefixes allowed for this BGP router. The range is from 1 to 4294967295.
	threshold	(OPTIONAL) Enter a number to be used as a percentage of the maximum value. When the number of prefixes reaches this percentage of the maximum value, the software sends a message. The range is from 1 to 100 percent. The default is **75**.
	warning-only	(OPTIONAL) Enter the keyword `warning-only` to set the router to send a log message when the maximum value is reached. If this parameter is not set, the router stops peering when the maximum number of prefixes is reached.

Defaults	threshold = **75**
Command Modes	ROUTER BGPV6-ADDRESS FAMILY
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	If you configure the `neighbor maximum-prefix` command and the neighbor receives more prefixes than allowed by the `neighbor maximum-prefix` command configuration, the neighbor goes down and the `show ip bgp ipv6 unicast summary` command displays (`prfxd`) in the State/PfxRcd column for that neighbor. The neighbor remains down until you enter the `capture bgp-pdu max-buffer-size` command for the neighbor or the peer group to which the neighbor belongs or you enter `neighbor shutdown` and `neighbor no shutdown` commands.
Related Commands	show ip bgp ipv6 unicast summary — displays the current BGP configuration.

neighbor X:X:X::X password

Enable TCP MD5 Authentication for an IPv6 BGP peer session.

Syntax	`neighbor x:x:x::x password {7 <encrypt-pass> | <clear-pass}` To return to the default setting, use the `no neighbor x:x:x::x password` command.
Parameters	*encrypt-pass* Enter the encrypted password. *clear-pass* Enter the clear text password.
Defaults	Disabled.
Command Modes	ROUTER BGPV6-ADDRESS FAMILY
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	The TCP session is authentication and prevents the data from being compromised.

neighbor next-hop-self

Allows you to configure the router as the next hop for a BGP neighbor. (This command is used for IBGP).

Syntax	`neighbor {`*`ipv6-address`*` | `*`peer-group-name`*`} next-hop-self` To return to the default setting, use the `no neighbor {`*`ipv6-address`*` | `*`peer-group-name`*`} next-hop-self` command.
Parameters	*ipv6-address*: Enter the IPv6 address in the x:x:x:x::x format. NOTE: The :: notation specifies successive hexadecimal fields of zeros. *peer-group-name*: (OPTIONAL) Enter the name of the peer group.
Defaults	Disabled.
Command Modes	ROUTER BGPV6-ADDRESS FAMILY
Command History	Version 9.2(0.0): Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	If you configure the `set ipv6 next-hop` command in ROUTE-MAP mode, its configuration takes precedence over the `neighbor next-hop-self` command.

neighbor peer-group (assigning peers)

Allows you to assign one peer to a existing peer group.

Syntax	`neighbor `*`ipv6-address`*` peer-group `*`peer-group-name`* To delete a peer from a peer group, use the `no neighbor `*`ipv6-address`*` peer-group `*`peer-group-name`* command.
Parameters	*ipv6-address*: Enter the IPv6 address in the x:x:x:x::x format. NOTE: The :: notation specifies successive hexadecimal fields of zeros. peer-group *peer-group-name*: Enter the keywords `peer-group` then the name of a configured peer group (maximum 16 characters).
Defaults	Not configured.
Command Modes	ROUTER BGP

Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

You can assign up to 64 peers to one peer group.

When you add a peer to a peer group, it inherits all the peer group's configured parameters. A peer cannot become part of a peer group if any of the following commands are configured on the peer:

- neighbor advertisement-interval
- neighbor distribute-list
- neighbor filter-list
- neighbor next-hop-self
- neighbor route-map
- neighbor route-reflector-client
- neighbor send-community

A neighbor may keep its configuration after it was added to a peer group if the neighbor's configuration is more specific than the peer group's and the neighbor's configuration does not affect outgoing updates.

A peer group must exist before you add a peer to it. If the peer group is disabled (`shutdown`) the peers within the group are also disabled (`shutdown`).

Related Commands

capture bgp-pdu max-buffer-size — resets BGP sessions.

neighbor peer-group (creating group) — creates a peer group.

show ip bgp ipv6 unicast peer-group — views BGP peers.

show ip bgp ipv6 unicast neighbors — views BGP neighbors configurations.

neighbor peer-group (creating group)

Allows you to create a peer group and assign it a name.

Syntax

`neighbor peer-group-name peer-group`

To delete a peer group, use the `no neighbor peer-group-name peer-group` command.

Parameters

peer-group-name	Enter a text string up to 16 characters long as the name of the peer group.

Defaults

Not configured.

Command Modes	ROUTER BGP
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	When a peer group is created, it is disabled (`shut mode`).
Related Commands	neighbor peer-group (assigning peers) — assigns routers to a peer group. neighbor remote-as — assigns a indirectly connected AS to a neighbor or peer group. neighbor shutdown — disables a peer or peer group.

neighbor peer-group passive

Enable passive peering on a BGP peer group; that is, the peer group does not send an OPEN message, but does respond to one.

Syntax	`neighbor` *`peer-group-name`* `peer-group passive` To delete a passive peer-group, use the `no neighbor` *`peer-group-name`* `peer-group passive` command.
Parameters	***peer-group-name*** Enter a text string up to 16 characters long as the name of the peer group.
Defaults	Not configured.
Command Modes	ROUTER BGP
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	After you configure a peer group as passive, you must assign it a subnet using the `neighbor subnet` command.
Related Commands	neighbor subnet — assigns a subnet to a dynamically configured BGP neighbor.

neighbor remote-as

Create and specify the remote peer to the BGP neighbor.

Syntax

`neighbor {ipv6-address | peer-group-name} remote-as number`

To delete a remote AS entry, use the `no neighbor {ipv6-address | peer-group-name} remote-as number` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. NOTE: The :: notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter a text string up to 16 characters long as the name of the peer group.
number	Enter a number of the AS. The range is from 1 to 65535.

Defaults

Not configured.

Command Modes

ROUTER BGP

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

If the `number` parameter is the same as the AS number used in the `router bgp` command, the remote AS entry in the neighbor is considered an internal BGP peer entry.

This command creates a peer and the newly created peer is disabled (`shutdown`).

Related Commands

router bgp — enters the ROUTER BGP mode and configure routes in an AS.

neighbor remove-private-as

Remove private AS numbers from the AS-PATH of outgoing updates.

Syntax

`neighbor {ipv6-address | peer-group-name} remove-private-as`

To return to the default, use the `no neighbor {ipv6-address | peer-group-name} remove-private-as` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. NOTE: The :: notation specifies successive hexadecimal fields of zeros.

peer-group-name	Enter the name of the peer group to remove the private AS numbers.

Defaults Disabled (that is, the private AS number are not removed).

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Applies to external border gateway protocol (EBGP) neighbors only.

If the AS-PATH contains both public and private AS number or contains AS numbers of an EBGP neighbor, the private AS numbers are not removed.

If a confederation contains private AS numbers in its AS-PATH, the software removes the private AS numbers only if they follow the confederation numbers in the AS path.

Private AS numbers are from 64512 to 65535.

neighbor route-map

Apply an established route map to either incoming or outbound routes of a BGP neighbor or peer group.

Syntax

```
neighbor {ipv6-address | peer-group-name} route-map map-name
{in | out}
```

To remove the route map, use the `no neighbor {ipv6-address | peer-group-name} route-map map-name {in | out}` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. NOTE: The :: notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group.
map-name	Enter the name of an established route map. If the Route map is not configured, the default is **deny** (to drop all routes).
in	Enter the keyword `in` to filter inbound routes.
out	Enter the keyword `out` to filter outbound routes.

Defaults Not configured.

Command Modes	ROUTER BGPV6-ADDRESS FAMILY
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	When you apply a route map to outbound routes, only routes that match at least one section of the route map are permitted. If you identify a peer group by name, the peers in that peer group inherit the characteristics in the Route map used in this command. If you identify a peer by IP address, the Route map overwrites either the inbound or outbound policies on that peer.

neighbor route-reflector-client

Configure a neighbor as a member of a route reflector cluster.

Syntax

```
neighbor {ipv6-address | peer-group-name} route-reflector-client
```

To indicate that the neighbor is not a route reflector client or to delete a route reflector configuration, use the `no neighbor {ipv6-address | peer-group-name} route-reflector-client` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group. All routers in the peer group receive routes from a route reflector.

Defaults	Not configured.
Command Modes	ROUTER BGPV6-ADDRESS FAMILY
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	The first time you enter this command it configures the neighbor as a route reflector and members of the route-reflector cluster. Internal BGP (IBGP) speakers do not need to be fully meshed if you configure a route reflector. When all clients of a route reflector are disabled, the neighbor is no longer a route reflector.

neighbor send-community

Send a COMMUNITY attribute to a BGP neighbor or peer group. A COMMUNITY attribute indicates that all routes with that attribute belong to the same community grouping.

Syntax `neighbor {`*`ipv6-address`*` | `*`peer-group-name`*`} send-community`

To disable sending a COMMUNITY attribute, use the `no neighbor {`*`ipv6-address`*` | `*`peer-group-name`*`} send-community` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. NOTE: The :: notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group. All routers in the peer group receive routes from a route reflector.

Defaults Not configured and COMMUNITY attributes are not sent to neighbors.

Command Modes ROUTER BGP

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

neighbor shutdown

Disable a BGP neighbor or peer group.

Syntax `neighbor {`*`ipv6-address`*` | `*`peer-group-name`*`} shutdown`

To enable a disabled neighbor or peer group, use the `no neighbor {`*`ipv6-address`*` | `*`peer-group-name`*`} shutdown` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. NOTE: The :: notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group to disable or enable all routers within the peer group.

Defaults Enabled (that is, BGP neighbors and peer groups are disabled.)

Command Modes ROUTER BGP

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information	Peers that are enabled within a peer group are disabled when their peer group is disabled. The `neighbor shutdown` command terminates all BGP sessions on the BGP neighbor or BGP peer group. Use this command with caution as it terminates the specified BGP sessions. When a neighbor or peer group is shutdown, use the `show ip bgp ipv6 unicast summary` command to confirm its status.
Related Commands	show ip bgp ipv6 unicast summary — displays the current BGP configuration. show ip bgp ipv6 unicast neighbors — displays IPv6 routing information exchanged by BGP neighbors.

neighbor soft-reconfiguration inbound

Enable a BGP soft-reconfiguration and start storing updates for inbound IPv6 unicast routes.

Syntax

```
neighbor {ipv4-address | ipv6-address | peer-group-name} soft-reconfiguration inbound
```

Parameters

ipv4-address | *ipv6-address*	Enter the IP address of the neighbor for which you want to start storing inbound routing updates.
peer-group-name	Enter the name of the peer group for which you want to start storing inbound routing updates.

Defaults	Disabled.
Command Modes	ROUTER BGPv6 ADDRESS FAMILY (conf-router_bgpv6_af)
Command History	Version 9.2(0.0) — Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	This command enables soft-reconfiguration for the specified BGP neighbor. BGP stores all updates for inbound IPv6 unicast routes the neighbor receives but does not reset the peer-session. △ **CAUTION: Inbound update storage is a memory-intensive operation. The entire BGP update database from the neighbor is stored in memory regardless of the inbound policy results applied on the neighbor.**
Related Commands	show ip bgp ipv6 unicast neighbors — displays IPv6 routing information BGP neighbors exchange.

neighbor subnet

Enable passive peering so that the members of the peer group are dynamic.

Syntax

`neighbor peer-group-name subnet subnet-number mask`

To remove passive peering, use the `no neighbor peer-group-name subnet subnet-number mask` command.

Parameters

subnet-number	Enter a subnet number in dotted decimal format (A.B.C.D.) as the allowable range of addresses included in the Peer group. To allow all addresses, enter `0::0/0`.
mask	Enter a prefix mask in / prefix-length format (/x).

Defaults Not configured.

Command Modes ROUTER BGP

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

neighbor timers

Set keepalive and hold time timers for a BGP neighbor or a peer group.

Syntax

`neighbor {ipv6-address | peer-group-name} timers keepalive holdtime`

To return to the default values, use the `no neighbor {ipv6-address | peer-group-name} timers` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. NOTE: The :: notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group to set the timers for all routers within the peer group.
keepalive	Enter a number for the time interval, in seconds, between keepalive messages sent to the neighbor routers. the range is from 1 to 65535. the default is **60 seconds**.
holdtime	Enter a number for the time interval, in seconds, between the last keepalive message and declaring the router dead. The range is from 3 to 65535. The default is **180 seconds**.

Defaults

- keepalive = **60 seconds**
- holdtime = **180 seconds**

Command Modes

ROUTER BGP

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Timer values configured with the `neighbor timers` command override the timer values configured with the `timers bgp` command.

When two neighbors, configured with different keepalive and holdtime values, negotiate for new values, the resulting values are as follows:

- the lower of the holdtime values is the new holdtime value
- whichever is the lower value; one-third of the new holdtime value, or the configured keepalive value is the new keepalive value

neighbor update-source

Enable the software to use Loopback interfaces for TCP connections for BGP sessions.

Syntax

```
neighbor {ipv6-address | peer-group-name} update-source
loopback interface
```

To use the closest interface, use the `no neighbor {ipv6-address | peer-group-name} update-source loopback interface` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. NOTE: The :: notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group to set the timers for all routers within the peer group.
loopback *interface*	Enter the keyword `loopback` then a number of the loopback interface. The range is from 0 to 16383.

Defaults

Not configured.

Command Modes

ROUTER BGP

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Loopback interfaces are up constantly and the BGP session may need one interface constantly up to stabilize the session. The `neighbor update-source` command is not necessary for directly connected internal BGP sessions.

neighbor weight

Assign a weight to the neighbor connection, which is used to determine the best path.

Syntax

`neighbor {`*`ipv6-address`*` | `*`peer-group-name`*`} weight `*`weight`*

To remove a weight value, use the `no neighbor {`*`ipv6-address`*` | `*`peer-group-name`*`} weight `*`weight`* command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. NOTE: The :: notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group to set the timers for all routers within the peer group.
weight	Enter a number as the weight. The range is from 0 to 65535. The default is **0**.

Defaults

0

Command Modes

ROUTER BGP

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

In the system best path selection process, the path with the highest weight value is preferred.

NOTE: To apply the weight to the connection and recompute the best path, reset the neighbor connection (the `capture bgp-pdu max-buffer-size *` command).

network

Specify the networks for the BGP process and enter them in the BGP routing table.

Syntax

`network `*`ipv6-address prefix-length`*` [route-map `*`map-name`*`]`

To remove a network, use the `no network `*`ip-address mask`*` [route-map `*`map-name`*`]` command.

Parameters

ipv6-address prefix-length	Enter the IPv6 address in the x:x:x:x::x format then the prefix length in the /x format. The range is from /0 to /128. NOTE: The :: notation specifies successive hexadecimal fields of zeros.
mask	Enter the mask of the IP address in the slash prefix length format (for example, /24). The mask appears in command outputs in dotted decimal format (A.B.C.D).
route-map *map-name*	(OPTIONAL) Enter the keywords `route-map` then the name of an established route map. If the route map is not configured, the default is **deny** (to drop all routes).

Defaults

Not configured.

Command Modes

ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The software resolves the network address configured by the `network` command with the routes in the main routing table to ensure that the networks are reachable using non-BGP routes and non-default routes.

Related Commands

redistribute — redistributes routes into BGP.

network backdoor

Specify this IGP route as the preferred route.

Syntax

`network ipv6-address prefix-length backdoor`

To remove a network, use the `no network ipv6-address prefix-length backdoor` command.

Parameters

ipv6-address prefix-length	Enter the IPv6 address in the x:x:x:x::x format then the prefix length in the /x format. The range is from /0 to /128. NOTE: The :: notation specifies successive hexadecimal fields of zeros.

Defaults

Not configured.

Command Modes	ROUTER BGPV6-ADDRESS FAMILY
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	Though the system does not generate a route due to backdoor config, there is an option for injecting/ sourcing a local route in presence of network backdoor config on a learned route.

redistribute

Redistribute routes into BGP.

Syntax

`redistribute {connected | static} [route-map map-name]`

To disable redistribution, use the `no redistribution {connected | static}` command.

Parameters

connected	Enter the keyword `connected` to redistribute routes from physically connected interfaces.
static	Enter the keyword `static` to redistribute manually configured routes. These routes are treated as incomplete routes.
route-map *map-name*	(OPTIONAL) Enter the keywords `route-map` then the name of an established route map. If the route map is not configured, the default is **deny** (to drop all routes).

Defaults	Not configured.
Command Modes	ROUTER BGPV6-ADDRESS FAMILY
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

If you do not configure the `default-metric` command, in addition to the `redistribute` command, or there is no route map to set the metric, the metric for redistributed static and connected is "0".

To redistribute the default route (`0::0/0`), configure the `neighbor default-originate` command.

Related Commands

neighbor default-originate — injects the default route.

redistribute isis

Redistribute IS-IS routes into BGP.

Syntax	`redistribute isis [level-1 | level-1-2 | level-2] [metric` *`metric-value`* `| metric-type {external | internal}] [route-map` *`map-name`*`]` To stop redistribution of IS-IS routes, use the `no redistribute isis` command.

Parameters

level-1 | level-1-2 | level-2]	(OPTIONAL) Enter the type (level) of routes to redistribute.
metric	(OPTIONAL) Assign metric to an interface for use with IPv6 information.
metric-type	(OPTIONAL) The external link type associated with the default route advertised into a routing domain. You must specify one of the following: • external • **internal** (default)
route-map *map-name*	(OPTIONAL) Enter the keywords `route-map` then the name of an established route map. If the route map is not configured, the default is **deny** (to drop all routes).

Defaults	Not configured.
Command Modes	ROUTER BGPV6-ADDRESS FAMILY
Command History	Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

redistribute ospf

Redistribute OSPFv3 routes into BGP.

Syntax	`redistribute ospf` *`process-id`* `[[match external {1 | 2}] [match internal]] [route-map` *`map-name`*`]` To stop redistribution of OSPF routes, use the `no redistribute ospf` *`process-id`* command.

Parameters

process-id	Enter the number of the OSPFv3 process. The range is from 1 to 65535.

match external {1 | 2}	(OPTIONAL) Enter the keywords `match external` to redistribute OSPF external routes. You can specify `1` or `2` to redistribute those routes only.
match internal	(OPTIONAL) Enter the keywords `match internal` to redistribute OSPFv3 internal routes only.
route-map *map-name*	(OPTIONAL) Enter the keywords `route-map` then the name of an established route map. If the route map is not configured, the default is **deny** (to drop all routes).

Defaults: Not configured.

Command Modes: ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information: When you enter the `redistribute ospf process-id` command without any other parameters, the system redistributes all OSPF internal routes, external type 1 routes, and external type 2 routes.

router bgp

Enter ROUTER BGP mode to configure and enable BGP.

Syntax: `router bgp as-number`

To disable BGP, use the `no router bgp as-number` command.

Parameters

as-*number*	Enter the AS number. The range is from 1 to 65535.

Defaults: Not enabled.

Command Modes: CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

show capture bgp-pdu neighbor

Display BGP packet capture information for an IPv6 address.

Syntax	`show capture bgp-pdu neighbor` *`ipv6-address`*
Parameters	*ipv6-address* — Enter the IPv6 address (X:X:X:X::X) of a BGP neighbor.
Defaults	EXEC EXEC Privilege
Command Modes	CONFIGURATION
Command History	**Version 9.2(0.0)** — Introduced on the MXL 10/40GbE Switch IO Module.
Related Command	capture bgp-pdu neighbor (ipv6) — enables capture of an IPv6 BGP neighbor packet. capture bgp-pdu max-buffer-size — specifies a size for the capture buffer.

show config

View the current ROUTER BGP configuration.

Syntax	`show config`
Command Modes	ROUTER BGPV6-ADDRESS FAMILY
Command History	**Version 9.2(0.0)** — Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell(conf-router_bgp)#show conf
!
router bgp 18508
 neighbor RR-CLIENT peer-group
 neighbor RR-CLIENT remote-as 18508
 neighbor RR-CLIENT no shutdown
 neighbor RR-CLIENT-PASSIV peer-group passive
 neighbor RR-CLIENT-PASSIV remote-as 18508
 neighbor RR-CLIENT-PASSIV subnet 9000::9:0/120
 neighbor RR-CLIENT-PASSIV no shutdown
 neighbor 1109::33 remote-as 18508
 neighbor 1109::33 update-source Loopback 101
 neighbor 1109::33 no shutdown
 neighbor 2222::220 remote-as 18508
 neighbor 2222::220 route-reflector-client
 neighbor 2222::220 update-source Loopback 100
 neighbor 2222::220 no shutdown
 neighbor 4000::33 remote-as 18508
 neighbor 4000::33 no shutdown
 neighbor 4000::60 remote-as 18508
 neighbor 4000::60 no shutdown
 neighbor 9000::1:2 remote-as 640
 no neighbor 9000::1:2 activate
 neighbor 9000::1:2 no shutdown

!
Dell#
```

show ip bgp ipv6 unicast

View the current BGP information.

Syntax `show ip bgp ipv6 unicast [`*`network`*` [`*`network-mask`*`] [longer-prefixes]]`

Paramters

network	(OPTIONAL) Enter the network address (in dotted decimal format) of the BGP network to view information only on that network.
network-mask	(OPTIONAL) Enter the keywords `network mask` (in slash prefix format) of the BGP network address.
longer-prefixes	(OPTIONAL) Enter the keywords `longer-prefixes` to view all routes with a common prefix.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information When you enable the `bgp non-deterministic-med` command, the `show ip bgp` command output for a BGP route does not list the INACTIVE reason.

show ip bgp ipv6 unicast cluster-list

View BGP neighbors in a specific cluster.

Syntax `show ip bgp ipv6 unicast cluster-list [`*`cluster-id`*`]`

Paramters

cluster-id	(OPTIONAL) Enter the cluster id in dotted decimal format.

Command Modes

- EXEC
- EXEC Privilege

Command History	Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

show ip bgp ipv6 unicast community

View information on all routes with community attributes or view specific BGP community groups.

Syntax

```
show ip bgp ipv6 unicast community [community-number] [local-
as] [no-export] [no-advertise]
```

Paramters

community-number	Enter the community number in AA:NN format where AA is the AS number (2 bytes) and NN is a value specific to that autonomous system. You can specify up to eight community numbers to view information on those community groups.
local-AS	Enter the keywords `local-AS` to view all routes with the COMMUNITY attribute of NO_EXPORT_SUBCONFED. All routes with the NO_EXPORT_SUBCONFED (0xFFFFFF03) community attribute must not be advertised to external BGP peers.
no-advertise	Enter the keywords `no-advertise` to view all routes containing the well-known community attribute of NO_ADVERTISE. All routes with the NO_ADVERTISE (0xFFFFFF02) community attribute must not be advertised to other BGP peers.
no-export	Enter the keywords `no-export` to view all routes containing the well-known community attribute of NO_EXPORT. All routes with the NO_EXPORT (0xFFFFFF01) community attribute must not be advertised outside a BGP confederation boundary.

Command Modes

- EXEC
- EXEC Privilege

Command History	Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To view the total number of COMMUNITY attributes found, use the `show ip bgp ipv6 unicast summary` command. The text line above the route table states the number of COMMUNITY attributes found.

show ip bgp ipv6 unicast community-list

View routes that are affected by a specific community list.

Syntax

`show ip bgp ipv6 unicast community-list` *`community-list-name`* `[exact-match]`

Paramters

community-list-name	Enter the name of a configured IP community list.
exact-match	(OPTIONAL) Enter the keywords `exact-match` to display only for an exact match of the communities.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

show ip bgp ipv6 unicast dampened-paths

View BGP routes that are dampened (non-active).

Syntax

`show ip bgp ipv6 unicast dampened-paths`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

show ip bgp ipv6 unicast detail

Display BGP internal information for IPv6 Unicast address family.

Syntax

`show ip bgp ipv6 unicast detail`

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History	Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

show ip bgp ipv6 unicast extcommunity-list

View information on all routes with Extended Community attributes.

Syntax `show ip bgp ipv6 unicast extcommunity-list [list name]`

Parameters

list name	Enter the extended community list name you wish to view.

Command Modes

- EXEC
- EXEC Privilege

Command History	Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To view the total number of COMMUNITY attributes found, use the `show ip bgp ipv6 unicast summary` command. The text line above the route table states the number of COMMUNITY attributes found.

The `show ip bgp ipv6 unicast community` command without any parameters lists BGP routes with at least one BGP community attribute and the output is the same as for the `show ip bgp ipv6 unicast` command output.

show ip bgp ipv6 unicast filter-list

View the routes that match the filter lists.

Syntax `show ip bgp ipv6 unicast filter-list as-path-name`

Parameters

as-path-name	Enter the name of an AS-PATH.

Command Modes

- EXEC
- EXEC Privilege

Command History	Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

show ip bgp ipv6 unicast flap-statistics

View flap statistics on BGP routes.

Syntax

`show ip bgp ipv6 unicast flap-statistics [ipv6-address prefix-length] [filter-list as-path-name] [regexp regular-expression]`

Parameters

ipv6-address prefix-length	Enter the IPv6 address in the x:x:x:x::x format then the prefix length in the /x format. The range is from /0 to /128. NOTE: The :: notation specifies successive hexadecimal fields of zeros.
filter-list *as-path-name*	(OPTIONAL) Enter the keywords `filter-list` then the name of a configured AS-PATH ACL.
regexp *regular-expression*	Enter a regular expression then use one or a combination of the following characters to match: • `.` = (period) any single character (including a white space). • `*` = (asterisk) the sequences in a pattern (0 or more sequences). • `+` = (plus) the sequences in a pattern (1 or more sequences). • `?` = (question mark) sequences in a pattern (either 0 or 1 sequences). NOTE: You must enter an escape sequence (CTRL+v) prior to entering the `?` regular expression. • `[ ]` = (brackets) a range of single-character patterns. • `^` = (caret) the beginning of the input string. If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified. • `$` = (dollar sign) the end of the output string.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

show ip bgp ipv6 unicast inconsistent-as

View routes with inconsistent originating autonomous system (AS) numbers; that is, prefixes that are announced from the same neighbor AS but with a different AS-Path.

Syntax

`show ip bgp ipv6 unicast inconsistent-as`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

show ip bgp ipv6 unicast neighbors

Displays information on IPv6 unicast routes exchanged by BGP neighbors.

Syntax

```
show ip bgp ipv6 unicast neighbors [ipv4-neighbor-addr | ipv6-neighbor-addr] [advertised-routes | dampened-routes | detail | flap-statistics | routes | received-routes [network [network-mask]] | denied-routes [network [network-mask]]]
```

Parameters

ipv6 unicast	Enter the keywords `ipv6 unicast` to view information only related to IPv6 unicast routes.
ipv4-neighbor-addr | *ipv6-neighbor-addr*	(OPTIONAL) Enter the IP address of the neighbor to view only BGP route information exchanged with that neighbor.
advertised-routes	(OPTIONAL) Enter the keywords `advertised-routes` to view only the routes the neighbor sent.
dampened-routes	(OPTIONAL) Enter the keywords `dampened-routes` to view information on dampened routes from the BGP neighbor.
detail	(OPTIONAL) Enter the keyword `detail` to view neighbor-specific internal information for the IPv4 Unicast address family.
flap-statistics	(OPTIONAL) Enter the keywords `flap-statistics` to view flap statistics on the neighbor's routes.
routes	(OPTIONAL) Enter the keyword `routes` to view only the neighbor's feasible routes.
received-routes [*network* [*network-mask*]	(OPTIONAL) Enter the keywords `received-routes` then either the network address (in dotted decimal format) or the network mask (in slash prefix format) to view all information received from neighbors. NOTE: You must configure the `neighbor soft-reconfiguration inbound` command prior to viewing all the information received from the neighbors.
denied-routes [*network* [*network-mask*]	(OPTIONAL) Enter the keywords `denied-routes` then either the network address (in dotted decimal format) or the network mask (in slash prefix format) to view all information on routes denied using neighbor inbound filters.

Command Modes	- EXEC - EXEC Privilege
Command History	Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show ip bgp ipv6 unicast neighbors` command shown in the Example below.

Lines Beginning With	Description
BGP neighbor	Displays the BGP neighbor address and its AS number. The last phrase in the line indicates whether the link between the BGP router and its neighbor is an external or internal one. If they are located in the same AS, then the link is internal; otherwise, the link is external.
BGP version	Displays the BGP version (always version 4) and the remote router ID.
BGP state	Displays the neighbor's BGP state and the amount of time in hours:minutes:seconds it has been in that state.
Last read	This line displays the following information: • last read is the time (hours:minutes:seconds) the router reads a message from its neighbor • hold time is the number of seconds configured between messages from its neighbor • keepalive interval is the number of seconds between keepalive messages to help ensure that the TCP session is still alive
Received messages	This line displays the number of BGP messages received, the number of notifications (error messages), and the number of messages waiting in a queue for processing.
Sent messages	The line displays the number of BGP messages sent, the number of notifications (error messages), and the number of messages waiting in a queue for processing.
Received updates	This line displays the number of BGP updates received and sent.
Soft reconfiguration	This line indicates that soft reconfiguration inbound is configured.
Minimum time	Displays the minimum time, in seconds, between advertisements.
(List of inbound and outbound policies)	Displays the policy commands configured and the names of the Route map, AS-PATH ACL, or Prefix list configured for the policy.

Lines Beginning With	Description
For address family:	Displays IPv6 Unicast as the address family.
BGP table version	Displays which version of the primary BGP routing table the router and the neighbor are using.
Prefixes accepted	Displays the number of network prefixes accepted by the router and the amount of memory used to process those prefixes.
Prefixes advertised	Displays the number of network prefixes advertised, the number rejected, and the number withdrawn from the BGP routing table.
Connections established	Displays the number of TCP connections established and dropped between the two peers to exchange BGP information.
Last reset	Displays the amount of time since the peering session was last reset. Also states if the peer resets the peering session. If the peering session was never reset, the word “never” is displayed.
Local host:	Displays the peering address of the local router and the TCP port number.
Foreign host:	Displays the peering address of the neighbor and the TCP port number.

Example

```
Dell#show ip bgp ipv6 unicast neighbors

BGP neighbor is 5ffe:10::3, remote AS 1, external link
  BGP version 4, remote router ID 5.5.5.3
  BGP state ESTABLISHED, in this state for 00:00:32
  Last read 00:00:32, last write 00:00:32
  Hold time is 180, keepalive interval is 60 seconds
  Received 1404 messages, 0 in queue
    3 opens, 1 notifications, 1394 updates
    6 keepalives, 0 route refresh requests
  Sent 48 messages, 0 in queue
    3 opens, 2 notifications, 0 updates
    43 keepalives, 0 route refresh requests
  Minimum time between advertisement runs is 30 seconds
  Minimum time before advertisements start is 0 seconds

  Capabilities received from neighbor for IPv6 Unicast :
    MULTIPROTO_EXT(1)
    ROUTE_REFRESH(2)
    CISCO_ROUTE_REFRESH(128)

  Capabilities advertised to neighbor for IPv6 Unicast :
    MULTIPROTO_EXT(1)
    ROUTE_REFRESH(2)
    CISCO_ROUTE_REFRESH(128)

  For address family: IPv6 Unicast
  BGP table version 12, neighbor version 12
  2 accepted prefixes consume 32 bytes

  Prefixes accepted 1 (consume 4 bytes), withdrawn 0 by peer
  Prefixes advertised 0, rejected 0, withdrawn 0 from peer
  Connections established 3; dropped 2
  Last reset 00:00:39, due to Closed by neighbor

  Notification History
    'OPEN error/Bad AS' Sent : 0 Recv: 1

  Local host: 5ffe:10::4, Local port: 179
  Foreign host: 5ffe:10::3, Foreign port: 35470

  Notification History
    'Connection Reset' Sent : 1 Recv: 0

  BGP neighbor is 5ffe:11::3, remote AS 1, external link
    BGP version 4, remote router ID 5.5.5.3
    BGP state ESTABLISHED, in this state for 00:00:28
    Last read 00:00:28, last write 00:00:28
    Hold time is 180, keepalive interval is 60 seconds
    Received 27 messages, 3 notifications, 0 in queue
    Sent 0 messages, 0 notifications, 0 in queue
    Received 8 updates, Sent 0 updates
    Route refresh request: received 0, sent 0
    Minimum time between advertisement runs is 30 seconds
    Minimum time before advertisements start is 0 seconds

  Capabilities received from neighbor for IPv6 Unicast :
    MULTIPROTO_EXT(1)
    ROUTE_REFRESH(2)
    CISCO_ROUTE_REFRESH(128)
    Capabilities advertised to neighbor for IPv6 Unicast :
    MULTIPROTO_EXT(1)
    ROUTE_REFRESH(2)
    CISCO_ROUTE_REFRESH(128)

  For address family: IPv6 Unicast
  BGP table version 12, neighbor version 12
  2 accepted prefixes consume 32 bytes

  Prefix advertised 0, rejected 0, withdrawn 0
  Connections established 3; dropped 2
  Last reset 00:00:41, due to Closed by neighbor

  Notification History
    'OPEN error/Bad AS' Sent : 0 Recv: 1

Local host: 5ffe:11::4, Local port: 179
```

show ip bgp ipv6 unicast peer-group

Allows you to view information on the BGP peers in a peer group.

Syntax	`show ip bgp ipv6 unicast peer-group [`*peer-group-name*` [summary]]`

Parameters

peer-group-name	(OPTIONAL) Enter the name of a peer group to view information about that peer group only.
detail	(OPTIONAL) Enter the keyword `detail` to view peer-group-specific information for the IPv6 address family.
summary	(OPTIONAL) Enter the keyword `summary` to view status information of the peers in that peer group. The output is the same as that found in the `show ip bgp ipv6 unicast summary` command.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show ip bgp peer-group

Peer-group RR-CLIENT, remote AS 18508
  BGP version 4
  Minimum time between advertisement runs is 5 seconds

  For address family: IPv4 Unicast
  BGP neighbor is RR-CLIENT, peer-group internal,
  Number of peers in this group 1
  Peer-group members (* - outbound optimized):
    9000::4:

Peer-group RR-CLIENT-PASSIV, remote AS 18508
  BGP version 4
  Minimum time between advertisement runs is 5 seconds

  For address family: IPv4 Unicast
  BGP neighbor is RR-CLIENT-PASSIV, peer-group internal,
  Number of peers in this group 1
  Peer-group members (* - outbound optimized):
    9000::9:2*
Dell#
```

show ip bgp ipv6 unicast summary

Allows you to view the status of all BGP connections.

Syntax `show ip bgp ipv6 unicast summary`

Command Modes

- EXEC
- EXEC Privilege

Command History	
Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell# show ip bgp summary
BGP router identifier 55.55.55.55, local AS number 18508
BGP table version is 0, main routing table version 0
6 BGP path attribute entrie(s) using 392 bytes of memory
6 BGP AS-PATH entrie(s) using 294 bytes of memory
6 BGP community entrie(s) using 234 bytes of memory

Neighbor  AS    MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/
Pfx

1109::33   18508 0       0       0      0     0   never  Active
2222::220  18508 0       0       0      0     0   never  Active
4000::33   18508 0       0       0      0     0   never  Active
4000::60   18508 0       0       0      0     0   never  Active
9000::4:2  18508 0       0       0      0     0   never  Active
9000::5:2  1     35      32      0      0     0   00:16:42    0
9000::6:2  2     35      32      0      0     0   00:16:39    0
9000::7:2  3     35      32      0      0     0   00:16:41    0
9000::8:2  18508 35      32      0      0     0   00:16:42    0
9000::9:2  18508 44      19      0      0     0   00:16:41    0
9000::a:2  18508 35      32      0      0     0   00:16:43    0
9000::b:14 18508 29      29      0      0     0   00:13:01    0
Dell#
```

show ip bgp next-hop

View all next hops (using learned routes only) with current reachability and flap status. This command only displays one path, even if the next hop is reachable by multiple paths.

Syntax

```
show ip bgp next-hop [local-routes]
```

Parameters

local-routes	(OPTIONAL) Show next-hop information for local routes.

Command Modes

- EXEC
- EXEC Privilege

Command History	
Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show ip bgp next-hop
Next-hop   Via              RefCount Cost Flaps Time Elapsed
9000::5:2  9000::5:2, Gi 8/38  2        0    0   00:23:22
9000::6:2  9000::6:2, Gi 8/38  2        0    0   00:23:22
9000::7:2  9000::7:2, Gi 8/38  2        0    0   00:23:22
9000::8:2  9000::8:2, Gi 8/38  2        0    0   00:23:22
9000::9:2  9000::9:2, Gi 8/38  6000     0    0   00:23:16
9000::a:2  9000::a:2, Gi 8/38  2        0    0   00:23:22
Dell#
```

show ip bgp paths

View all the BGP path attributes in the BGP database.

Syntax

```
show ip bgp paths [regexp regular-expression]
```

Parameters

regexp ***regular-expression***

Enter a regular expression then use one or a combination of the following characters to match:

- `.` = (period) any single character (including a white space).
- `*` = (asterisk) the sequences in a pattern (0 or more sequences).
- `+` = (plus) the sequences in a pattern (1 or more sequences).
- `?` = (question mark) sequences in a pattern (either 0 or 1 sequences).

  NOTE: You must enter an escape sequence (CTRL+v) prior to entering the `?` regular expression.
- `[ ]` = (brackets) a range of single-character patterns.
- `^` = (caret) the beginning of the input string. If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified.
- `$` = (dollar sign) the end of the output string.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

show ip bgp paths as-path

View all unique AS-PATHs in the BGP database.

Syntax

```
show ip bgp paths as-path
```

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

show ip bgp paths community

View all unique COMMUNITY numbers in the BGP database.

Syntax `show ip bgp paths community`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

show ip bgp paths extcommunity

View all unique extended community information in the BGP database.

Syntax `show ip bgp paths extcommunity`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

show ip bgp regexp

Allows you to view the subset of BGP routing table matching the regular expressions specified.

Syntax `show ip bgp regexp regular-expression [character]`

Parameters

regular-expression [character]

Enter a regular expression then use one or a combination of the following characters to match:

- `.` = (period) any single character (including a white space).
- `*` = (asterisk) the sequences in a pattern (0 or more sequences).
- `+` = (plus) the sequences in a pattern (1 or more sequences).
- `?` = (question mark) sequences in a pattern (either 0 or 1 sequences).

  NOTE: You must enter an escape sequence (CTRL+v) prior to entering the `?` regular expression.
- `[ ]` = (brackets) a range of single-character patterns.

- `^` = (caret) the beginning of the input string. If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified.
- `$` = (dollar sign) the end of the output string.

Command Modes	- EXEC - EXEC Privilege
Command History	Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

timers bgp

Allows you to adjust the BGP network timers for all neighbors.

Syntax

`timers bgp` *`keepalive holdtimer`*

To return to the default values, use the `no timers bgp` command.

Parameters

keepalive	Enter the time interval (in seconds) between which the system sends keepalive messages. The range is from 1 to 65535. The default is **60 seconds**.
holdtimer	Enter the time interval (in seconds) that the the system waits since the last keepalive message before declaring a BGP peer dead. The range is from 3 to 65535. The default is **180 seconds**.

Defaults

- keepalive = **60 seconds**
- holdtimer = **180 seconds**

Command Modes

ROUTER BGP

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

neighbor timers — adjusts BGP timers for a specific peer or peer group.

IPv6 MBGP Commands

Multiprotocol BGP (MBGP) is an enhanced BGP that enables multicast routing policy throughout the Internet and connecting multicast topologies between BGP and autonomous systems (AS). The Dell Networking MBGP is implemented as per IETF RFC 1858.

address family

This command changes the context to subsequent address family identifier (SAFI).

Syntax

```
address family ipv6 unicast
```

To remove SAFI context, use the `no address family ipv6 unicast` command.

Parameters

ipv6	Enter the keyword `ipv6` to specify the address family as IPv6.
unicast	Enter the keyword `unicast` to specify multicast as SAFI.

Defaults

IPv6 Unicast

Command Modes

ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

After this command is executed, all subsequent commands apply to this address family. You can exit from this AFI/SAFI to the IPv6 Unicast (the default) family by entering the `exit` command and returning to the Router BGP context.

aggregate-address

Summarize a range of prefixes to minimize the number of entries in the routing table.

Syntax

```
aggregate-address ipv6-address prefix-length [advertise-map
map-name] [as-set] [attribute-map map-name] [summary-only]
[suppress-map map-name]
```

Parameters

ipv6-address prefix-length	Enter the IPv6 address in the x:x:x:x::x format then the prefix length in the / x format. The range is from /0 to /128. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.

advertise-map *map-name*	(OPTIONAL) Enter the keywords `advertise-map` then the name of a configured route map to set filters for advertising an aggregate route.
as-set	(OPTIONAL) Enter the keywords `as-set` to generate path attribute information and include it in the aggregate. AS_SET includes AS_PATH and community information from the routes included in the aggregated route.
attribute-map *map-name*	(OPTIONAL) Enter the keywords `attribute-map` then the name of a configured route map to modify attributes of the aggregate, excluding AS_PATH and NEXT_HOP attributes.
summary-only	(OPTIONAL) Enter the keywords `summary-only` to advertise only the aggregate address. Specific routes are not advertised.
suppress-map *map-name*	(OPTIONAL) Enter the keywords `suppress-map` then the name of a configured route map to identify which more-specific routes in the aggregate are suppressed.

Defaults

Not configured.

Command Modes

ROUTER-BGPV6-ADDRESS FAMILY

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

At least one of the routes included in the aggregate address must be in the BGP routing table for the configured aggregate to become active.

Do not add the `as-set` parameter to the aggregate. If routes within the aggregate are constantly changing, the aggregate flaps to keep track of the changes in the AS_PATH.

In route maps used in the `suppress-map` parameter, routes meeting the `deny` clause are not suppress; in other words, they are allowed. The opposite is true: routes meeting the `permit` clause are suppressed.

If the route is injected using the `network` command, that route stills appear in the routing table if the `summary-only` parameter is configured in the `aggregate-address` command.

The `summary-only` parameter suppresses all advertisements. If you want to suppress advertisements to only specific neighbors, use the `neighbor distribute-list` command.

bgp dampening

Enable MBGP route dampening.

Syntax `bgp dampening [half-life time] [route-map map-name]`

To disable route dampening, use the `no bgp dampening [half-life time] [route-map map-name]` command.

Parameters

half-life time	(OPTIONAL) Enter the number of minutes after which the Penalty is decreased. After the router assigns a Penalty of 1024 to a route, the Penalty is decreased by half, after the half-life period expires. The range is from 1 to 45. The default is **15 minutes**.
route-map *map-name*	(OPTIONAL) Enter the keywords `route-map` then the name of a configured route map. Only match commands in the configured route map are supported.

Defaults Disabled.

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

clear ip bgp ipv6 unicast

Reset MBGP sessions.

Syntax `clear ip bgp ipv6 unicast * ipv6-address prefix-length [dampening | flap-statistics] peer-group]`

Parameters

*	Enter the character * to clear all peers.
ipv6-address prefix-length	Enter the IPv6 address in the x:x:x:x::x format then the prefix length in the /x format. The range is from /0 to /128. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
dampening	(OPTIONAL) Enter the keyword `dampening` to clear route flap dampening information.
flap-statistics	(OPTIONAL) Enter the keywords `flap-statistics` to reset the flap statistics on all prefixes from that neighbor.
peer-group	(OPTIONAL) Enter the keywords `peer-group` to clear all members of a peer-group.

Command Modes	EXEC Privilege	
Command History	Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

clear ip bgp ipv6 unicast dampening

Clear information on route dampening.

Syntax	`clear ip bgp dampening ipv6 unicast [`*`network network-mask`*`]`	
Parameters	*network*	(OPTIONAL) Enter the IPv6 network address in x:x:x:x::x format.
	network-mask	If you enter the network address, next enter the network mask, from 0 to 128.
Command Modes	EXEC Privilege	
Command History	Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

clear ip bgp ipv6 unicast flap-statistics

Clear BGP flap statistics, which includes the number of flaps and the time of the last flap.

Syntax	`clear ip bgp ipv6 unicast flap-statistics [`*`network`*`	filter-list `*`list`*` |regexp `*`regexp`*	
Parameters	*network*	(OPTIONAL) Enter the IPv6 network address in x:x:x:x::x format to clear flap statistics.
	filter-list *list*	(OPTIONAL) Enter the keywords `filter-list` then the name of a configured AS-PATH list (maximum 16 characters).
	regexp *regexp*	(OPTIONAL) Enter the keyword `regexp` then regular expressions. Use one or a combination of the following: • **.** (period) matches on any single character, including white space. • `*` (asterisk) matches on sequences in a pattern (zero or more sequences). • + (plus sign) matches on sequences in a pattern (one or more sequences). • `?` (question mark) matches sequences in a pattern (0 or 1 sequences).

- `[ ]` (brackets) matches a range of single-character patterns.
- `^` (caret) matches the beginning of the input string. (If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified.)
- `$` (dollar sign) matches the end of the output string.

Command Modes	EXEC Privilege
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.

debug ip bgp ipv6 unicast dampening

View information on routes being dampened.

Syntax `debug ip bgp ipv6 unicast dampening`

To disable debugging, use the `no debug ip bgp ipv6 unicast dampening` command.

Parameters

dampening	Enter the keyword `dampening` to clear route flap dampening information.

Command Modes EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the S4820T.

debug ip bgp ipv6 unicast peer-group updates

View information about BGP peer-group updates.

Syntax `debug ip bgp ipv6 unicast peer-group` *`peer-group-name`* `updates [in | out]`

To disable debugging, use the `no debug ip bgp ipv6 unicast peer-group` *`peer-group-name`* `updates [in | out]` command.

Parameters

peer-group *peer-group-name*	Enter the keywords `peer-group` then the name of the peer-group.

updates	Enter the keyword `updates` to view BGP update information.
in	(OPTIONAL) Enter the keyword `in` to view only BGP updates received from neighbors.
out	(OPTIONAL) Enter the keyword `out` to view only BGP updates sent to neighbors.

Command Modes EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

debug ip bgp ipv6 unicast updates

View information about BGP updates.

Syntax

```
debug ip bgp ipv6 unicast ipv6-address prefix-length updates
[in | out]
```

Parameters

ipv6-address prefix-length	Enter the IPv6 address in the x:x:x:x::x format then the prefix length in the /x format. The range is from /0 to /128. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
updates	Enter the keyword `updates` to view BGP update information.
in	(OPTIONAL) Enter the keyword `in` to view only BGP updates received from neighbors.
out	(OPTIONAL) Enter the keyword `out` to view only BGP updates sent to neighbors.

Defaults Disabled.

Command Modes EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

distance bgp

Define an administrative distance for routes.

Syntax

`distance bgp external-distance internal-distance local-distance`

To return to default values, use the `no distance bgp` command.

Parameters

external-distance	Enter a number to assign to routes learned from a neighbor external to the AS. The range is from 1 to 255. The default is **20**.
internal-distance	Enter a number to assign to routes learned from a router within the AS. The range is from 1 to 255. The default is **200**.
local-distance	Enter a number to assign to routes learned from networks listed in the network command. The range is from 1 to 255. The default is **200**.

Defaults

- external-distance = **20**
- internal-distance = **200**
- local-distance = **200**

Command Modes

ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

CAUTION: Dell Networking recommends that you do not change the administrative distance of internal routes. Changing the administrative distances may cause routing table inconsistencies.

The higher the administrative distance assigned to a route means that your confidence in that route is low. Routes assigned an administrative distance of 255 are not installed in the routing table.

Routes from confederations are treated as internal BGP routes.

neighbor activate

Allows you to enable a specified neighbor/peer group for the current address and subsequent address family identifier (AFI/SAFI).

Syntax

`neighbor [ipv6-address | peer-group-name] activate`

To disable, use the `no neighbor [ipv6-address | peer-group-name] activate` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. NOTE: The :: notation specifies successive hexadecimal fields of zeros.
peer-group-name	Identify a peer group by name.
activate	Enter the keyword `activate` to enable the identified neighbor or peer group in the new AFI/SAFI.

Defaults Disabled.

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information By default, when a neighbor/peer group configuration is created in the Router BGP context, it is enabled for the IPv6/Unicast AFI/SAFI. By using `activate` in the new context, the neighbor/peer group is enabled for AFI/SAFI.

Related Command address family — changes the context to SAFI.

neighbor advertisement-interval

Set the advertisement interval between BGP neighbors or within a BGP peer group.

Syntax

```
neighbor {ipv6-address | peer-group-name} advertisement-interval seconds
```

To return to the default value, use the `no neighbor {ipv6-address | peer-group-name} advertisement-interval` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. NOTE: The :: notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group to set the advertisement interval for all routers in the peer group.
seconds	Enter a number as the time interval, in seconds, between BGP advertisements. The range is from 0 to 600 seconds. The default is **5 seconds** for internal BGP peers and **30 seconds** for external BGP peers.

Defaults

- seconds = **5 seconds** (internal peers)

- seconds = **30 seconds** (external peers)

Command Modes

ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

neighbor default-originate

Inject the default route to a BGP peer or neighbor.

Syntax

`neighbor {ipv6-address | peer-group-name} default-originate [route-map map-name]`

To remove a default route, use the `no neighbor {ipv6-address | peer-group-name} default-originate` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. NOTE: The :: notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group to set the default route of all routers in that peer group.
route-map *map-name*	(OPTIONAL) Enter the keywords `route-map` then the name of a configured route map.

Defaults

Not configured.

Command Modes

ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

neighbor distribute-list

Distribute BGP information using an established prefix list.

Syntax

`neighbor {ipv6-address | peer-group-name} distribute-list prefix-list-name {in | out}`

To delete a neighbor distribution list, use the `no neighbor {ipv6-address | peer-group-name} distribute-list prefix-list-name {in | out}` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. NOTE: The :: notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group.
prefix-list-name	Enter the name of an established prefix list. If the prefix list is not configured, the default is **permit** (to allow all routes).
in	Enter the keyword in to distribute only inbound traffic.
out	Enter the keyword out to distribute only outbound traffic.

Defaults: Not configured.

Command Modes: ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

neighbor filter-list — assigns a AS-PATH list to a neighbor or peer group.

neighbor route-map — assigns a route map to a neighbor or peer group.

neighbor filter-list

Configure a BGP filter based on the AS-PATH attribute.

Syntax

```
neighbor [ipv6-address | peer-group-name] filter-list aspath
access-list-name [in | out]
```

To delete a BGP filter, use the `no neighbor [ipv6-address | peer-group-name] filter-list aspath access-list-name [in | out]` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. NOTE: The :: notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group to apply the filter to all routers in the peer group.
access-list-name	Enter the name of an established AS-PATH access list. If the AS-PATH access list is not configured, the default is **permit** (to allow routes).
in	Enter the keyword `in` to filter inbound BGP routes.

out	Enter the keyword `out` to filter outbound BGP routes.

Defaults: Not configured.

Command Modes: ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

neighbor maximum-prefix

Control the number of network prefixes received.

Syntax

`neighbor {ipv6-address | peer-group-name} maximum-prefix maximum [threshold] [warning-only]`

To return to the default values, use the `no neighbor {ipv6-address | peer-group-name} maximum-prefix maximum [threshold] [warning-only]` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group.
maximum	Enter a number as the maximum number of prefixes allowed for this BGP router. The range is from 1 to 4294967295.
threshold	(OPTIONAL) Enter a number to be used as a percentage of the maximum value. When the number of prefixes reaches this percentage of the maximum value, the software sends a message. The range is from 1 to 100 percent. The default is **75**.
warning-only	(OPTIONAL) Enter the keyword `warning-only` to set the router to send a log message when the maximum value is reached. If this parameter is not set, the router stops peering when the maximum number of prefixes is reached.

Defaults: threshold = **75**

Command Modes: ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

neighbor next-hop-self

Allows you to configure the router as the next hop for a BGP neighbor.

Syntax	`neighbor {ipv6-address | peer-group-name} next-hop-self` To return to the default setting, use the `no neighbor {ipv6-address | peer-group-name} next-hop-self` command.
Parameters	*ipv6-address*: Enter the IPv6 address in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros. *peer-group-name*: (OPTIONAL) Enter the name of the peer group.
Defaults	Disabled.
Command Modes	ROUTER BGPV6-ADDRESS FAMILY
Command History	Version 9.2(0.0) — Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	If you configure the `set ipv6 next-hop` command in ROUTE-MAP mode, its configuration takes precedence over the `neighbor next-hop-self` command.

neighbor remove-private-as

Remove private AS numbers from the AS-PATH of outgoing updates.

Syntax	`neighbor {ipv6-address | peer-group-name} remove-private-as` To return to the default, use the `no neighbor {ipv6-address | peer-group-name} remove-private-as` command.
Parameters	*ipv6-address*: Enter the IPv6 address in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros. *peer-group-name*: Enter the name of the peer group to remove the private AS numbers.
Defaults	Disabled (that is, the private AS number are not removed).
Command Modes	ROUTER BGPV6-ADDRESS FAMILY

Command History	**Version 9.2(0.0)**	Introduced on the MXL 10/40GbE Switch IO Module.

neighbor route-map

Apply an established route map to either incoming or outbound routes of a BGP neighbor or peer group.

Syntax

`neighbor {ipv6-address | peer-group-name} route-map map-name {in | out}`

To remove the route map, use the `no neighbor {ipv6-address | peer-group-name} route-map map-name {in | out}` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. NOTE: The :: notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group.
map-name	Enter the name of an established route map. If the Route map is not configured, the default is **deny** (to drop all routes).
in	Enter the keyword `in` to filter inbound routes.
out	Enter the keyword `out` to filter outbound routes.

Defaults

Not configured.

Command Modes

ROUTER BGPV6-ADDRESS FAMILY

Command History	**Version 9.2(0.0)**	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

When you apply a route map to outbound routes, only routes that match at least one section of the route map are permitted.

If you identify a peer group by name, the peers in that peer group inherit the characteristics in the Route map used in this command. If you identify a peer by IP address, the Route map overwrites either the inbound or outbound policies on that peer.

neighbor route-reflector-client

Configure a neighbor as a member of a route reflector cluster.

Syntax

`neighbor {ipv6-address | peer-group-name} route-reflector-client`

To indicate that the neighbor is not a route reflector client or to delete a route reflector configuration, use the `no neighbor {ipv6-address | peer-group-name} route-reflector-client` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group. All routers in the peer group receive routes from a route reflector.

Defaults

Not configured.

Command Modes

ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The first time you enter this command it configures the neighbor as a route reflector and members of the route-reflector cluster. Internal BGP (IBGP) speakers do not need to be fully meshed if you configure a route reflector.

When all clients of a route reflector are disabled, the neighbor is no longer a route reflector.

network

Specify the networks for the BGP process and enter them in the BGP routing table.

Syntax

`network ipv6-address [route-map map-name]`

To remove a network, use the `no network ipv6-address [route-map map-name]` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.

route-map *map-name*	(OPTIONAL) Enter the keywords `route-map` then the name of an established route map. If the route map is not configured, the default is **deny** (to drop all routes).

Defaults: Not configured.

Command Modes: ROUTER BGPV6-ADDRESS FAMILY

Command History:

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information: The software resolves the network address configured by the `network` command with the routes in the main routing table to ensure that the networks are reachable using non-BGP routes and non-default routes.

Related Commands: redistribute — redistributes routes into BGP.

redistribute

Redistribute routes into BGP.

Syntax: `redistribute {connected | static} [route-map map-name]`

To disable redistribution, use the `no redistribution {connected | static}` command.

Parameters:

connected	Enter the keyword `connected` to redistribute routes from physically connected interfaces.
static	Enter the keyword `static` to redistribute manually configured routes. These routes are treated as incomplete routes.
route-map *map-name*	(OPTIONAL) Enter the keywords `route-map` then the name of an established route map. If the route map is not configured, the default is **deny** (to drop all routes).

Defaults: Not configured.

Command Modes: ROUTER BGPV6-ADDRESS FAMILY

Command History:

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information	If you do not configure the `default-metric` command, in addition to the `redistribute` command, or there is no route map to set the metric, the metric for redistributed static and connected is "0". To redistribute the default route (`0::0/0`), configure the `neighbor default-originate` command.
Related Commands	neighbor default-originate — injects the default route.

show ip bgp ipv6 unicast

View the current BGP information.

Syntax `show ip bgp ipv6 unicast [network [network-mask] [longer-prefixes]]`

Paramters

network	(OPTIONAL) Enter the network address (in dotted decimal format) of the BGP network to view information only on that network.
network-mask	(OPTIONAL) Enter the keywords `network mask` (in slash prefix format) of the BGP network address.
longer-prefixes	(OPTIONAL) Enter the keywords `longer-prefixes` to view all routes with a common prefix.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information When you enable the `bgp non-deterministic-med` command, the `show ip bgp` command output for a BGP route does not list the INACTIVE reason.

show ip bgp ipv6 unicast cluster-list

View BGP neighbors in a specific cluster.

Syntax `show ip bgp ipv6 unicast cluster-list [cluster-id]`

Paramters

cluster-id	(OPTIONAL) Enter the cluster id in dotted decimal format.

Command Modes	- EXEC - EXEC Privilege
Command History	Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

show ip bgp ipv6 unicast community

View information on all routes with community attributes or view specific BGP community groups.

Syntax

```
show ip bgp ipv6 unicast community [community-number] [local-
as] [no-export] [no-advertise]
```

Paramters

community-number	Enter the community number in AA:NN format where AA is the AS number (2 bytes) and NN is a value specific to that autonomous system. You can specify up to eight community numbers to view information on those community groups.
local-AS	Enter the keywords `local-AS` to view all routes with the COMMUNITY attribute of NO_EXPORT_SUBCONFED. All routes with the NO_EXPORT_SUBCONFED (0xFFFFFF03) community attribute must not be advertised to external BGP peers.
no-advertise	Enter the keywords `no-advertise` to view all routes containing the well-known community attribute of NO_ADVERTISE. All routes with the NO_ADVERTISE (0xFFFFFF02) community attribute must not be advertised to other BGP peers.
no-export	Enter the keywords `no-export` to view all routes containing the well-known community attribute of NO_EXPORT. All routes with the NO_EXPORT (0xFFFFFF01) community attribute must not be advertised outside a BGP confederation boundary.

Command Modes	- EXEC - EXEC Privilege	
Command History	Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To view the total number of COMMUNITY attributes found, use the `show ip bgp ipv6 unicast summary` command. The text line above the route table states the number of COMMUNITY attributes found.

show ip bgp ipv6 unicast community-list

View routes that are affected by a specific community list.

Syntax	`show ip bgp ipv6 unicast community-list` *`community-list-name`*
Paramters	

community-list-name	Enter the name of a configured IP community list.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

show ip bgp ipv6 unicast dampened-paths

View BGP routes that are dampened (non-active).

Syntax

```
show ip bgp ipv6 unicast dampened-paths
```

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

show ip bgp ipv6 unicast detail

Display detailed BGP information.

Syntax

```
show ip bgp ipv6 unicast detail
```

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
R2_Training#show ip bgp ipv6 unicast detail

Detail information for BGP Node
bgpNdP 0x41a17000 : NdTmrP 0x41a17000 : NdKATmrP 0x41a17014 :
NdTics 327741 :
NhLocAS 1 : NdState 2 : NdRPMPrim 1 : NdListSoc 13
```

```
NdAuto 1 : NdEqCost 1 : NdSync 0 : NdDefOrg 0
NdV6ListSoc 14 NdDefDid 0 : NdConfedId 0 : NdMedConfed 0 :
NdMedMissVal -1 :
NdIgnrIllId 0 : NdRRC2C 1 : NdClstId 33686273 : NdPaTblP
0x41a19088
NdASPTblP 0x41a19090 : NdCommTblP 0x41a19098 : NhOptTransTblP
0x41a190a0 :
NdRRClsTblP 0x41a190a8
NdPktPA 0 : NdLocCBP 0x41a6f000 : NdTmpPAP 0x419efc80 :
NdTmpASPAP 0x41a25000 :
NdTmpCommP 0x41a25800
NdTmpRRClP 0x41a4b000 : NdTmpOptP 0x41a4b800 : NdTmpNHP :
NdOrigPAP 0
NdOrgNHP 0 : NdModPathP 0x419efcc0 : NdModASPAP 0x41a4c000 :
NdModCommP 0x41a4c800
NdModOptP 0x41a4d000 : NdModNHP : NdComSortBufP 0x41a19110 :
NdComSortHdP
0x41a19d04 : NdUpdAFMsk 0 : AFRstSe
t 0x41a1a298 : NHopDfrdHdP 0x41a1a3e0 : NumNhDfrd 0 :
CfgHdrAFMsk 1
```

show ip bgp ipv6 unicast filter-list

View the routes that match the filter lists.

Syntax `show ip bgp ipv6 unicast filter-list` *`as-path-name`*

Parameters

as-path-name	Enter the name of an AS-PATH.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

show ip bgp ipv6 unicast flap-statistics

View flap statistics on BGP routes.

Syntax `show ip bgp ipv6 unicast flap-statistics [`*`ipv6-address prefix-length`*`] [`*`filter-list as-path-name`*`] [regexp `*`regular-expression`*`]`

Parameters

ipv6-address prefix-length	Enter the IPv6 address in the x:x:x:x::x format then the prefix length in the /x format. The range is from /0 to /128. NOTE: The :: notation specifies successive hexadecimal fields of zeros.

filter-list *as-path-name*	(OPTIONAL) Enter the keywords `filter-list` then the name of a configured AS-PATH ACL.
regexp *regular-expression*	Enter a regular expression then use one or a combination of the following characters to match: • `.` = (period) any single character (including a white space). • `*` = (asterisk) the sequences in a pattern (0 or more sequences). • `+` = (plus) the sequences in a pattern (1 or more sequences). • `?` = (question mark) sequences in a pattern (either 0 or 1 sequences). **NOTE**: You must enter an escape sequence (CTRL+v) prior to entering the `?` regular expression. • `[ ]` = (brackets) a range of single-character patterns. • `^` = (caret) the beginning of the input string. If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified. • `$` = (dollar sign) the end of the output string.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show ip bgp ipv6 unicast flap-statistics
BGP table version is 8, local router ID is 5.5.10.4
Status codes: s suppressed, S stale, d damped, h history, *
valid, > best Path
source: I - internal, a - aggregate, c - confed-external, r -
redistributed, n -
network Origin codes: i - IGP, e - EGP, ? - incomplete

   Network       From        Flaps  Duration Reuse Path
h  dead:1::/100  5ffe:10::3  1      00:03:20       1 i
h  dead:1::/100  5ffe:11::3  1      00:03:20       1 i
h  dead:4::/100  5ffe:10::3  1      00:04:39       1 i
h  dead:4::/100  5ffe:11::3  1      00:04:39       1 i

Dell#
```

show ip bgp ipv6 unicast inconsistent-as

View routes with inconsistent originating autonomous system (AS) numbers; that is, prefixes that are announced from the same neighbor AS but with a different AS-Path.

Syntax

```
show ip bgp ipv6 unicast inconsistent-as
```

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

show ip bgp ipv6 unicast neighbors

Allows you to view the information exchanged by BGP neighbors.

Syntax

```
show ip bgp ipv6 unicast neighbors [ipv6-address prefix-length
[advertised-routes | dampened-routes | detail | flap-statistics
| routes]]
```

Parameters

ipv6-address prefix-length	(OPTIONAL) Enter the IPv6 address in the x:x:x:x::x format then the prefix length in the /x format. The range is from /0 to /128. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
advertised-routes	(OPTIONAL) Enter the keywords `advertised-routes` to view only the routes the neighbor sent.
dampened-routes	(OPTIONAL) Enter the keywords `dampened-routes` to view information on dampened routes from the BGP neighbor.
flap-statistics	(OPTIONAL) Enter the keywords `flap-statistics` to view flap statistics on the neighbor's routes.
detail	(OPTIONAL) Display detailed neighbor information.
routes	(OPTIONAL) Enter the keyword `routes` to view only the neighbor's feasible routes.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show ip bgp ipv6 unicast neighbors` command shown in the Example below.

Lines Beginning With	Description
BGP neighbor	Displays the BGP neighbor address and its AS number. The last phrase in the line indicates whether the link between the BGP router and its neighbor is an external or internal one. If they are located in the same AS, then the link is internal; otherwise, the link is external.
BGP version	Displays the BGP version (always version 4) and the remote router ID.
BGP state	Displays the neighbor's BGP state and the amount of time in hours:minutes:seconds it has been in that state.
Last read	This line displays the following information: • last read is the time (hours:minutes:seconds) the router reads a message from its neighbor • hold time is the number of seconds configured between messages from its neighbor • keepalive interval is the number of seconds between keepalive messages to help ensure that the TCP session is still alive
Received messages	This line displays the number of BGP messages received, the number of notifications (error messages), and the number of messages waiting in a queue for processing.
Sent messages	The line displays the number of BGP messages sent, the number of notifications (error messages), and the number of messages waiting in a queue for processing.
Received updates	This line displays the number of BGP updates received and sent.
Minimum time	Displays the minimum time, in seconds, between advertisements.
(List of inbound and outbound policies)	Displays the policy commands configured and the names of the Route map, AS-PATH ACL, or Prefix list configured for the policy.
For address family:	Displays IPv6 Unicast as the address family.
BGP table version	Displays which version of the primary BGP routing table the router and the neighbor are using.
Accepted Prefixes	Displays the number of network prefixes accepted by the router and the amount of memory used to process those prefixes.

Lines Beginning With	Description
Prefixes advertised	Displays the number of network prefixes advertised, the number rejected, and the number withdrawn from the BGP routing table.
Connections established	Displays the number of TCP connections established and dropped between the two peers to exchange BGP information.
Last reset	Displays the amount of time since the peering session was last reset. Also states if the peer resets the peering session. If the peering session was never reset, the word "never" is displayed.
Local host:	Displays the peering address of the local router and the TCP port number.
Foreign host:	Displays the peering address of the neighbor and the TCP port number.

Example

```
Dell#show ip bgp ipv6 unicast neighbors

BGP neighbor is 5ffe:10::3, remote AS 1, external link
  BGP version 4, remote router ID 5.5.5.3
  BGP state ESTABLISHED, in this state for 00:00:32
  Last read 00:00:32, last write 00:00:32
  Hold time is 180, keepalive interval is 60 seconds
  Received 1404 messages, 0 in queue
    3 opens, 1 notifications, 1394 updates
    6 keepalives, 0 route refresh requests
  Sent 48 messages, 0 in queue
    3 opens, 2 notifications, 0 updates
    43 keepalives, 0 route refresh requests
  Minimum time between advertisement runs is 30 seconds
  Minimum time before advertisements start is 0 seconds

  Capabilities received from neighbor for IPv6 Unicast :
    MULTIPROTO_EXT(1)
    ROUTE_REFRESH(2)
    CISCO_ROUTE_REFRESH(128)

  Capabilities advertised to neighbor for IPv6 Unicast :
    MULTIPROTO_EXT(1)
    ROUTE_REFRESH(2)
    CISCO_ROUTE_REFRESH(128)

  For address family: IPv6 Unicast
  BGP table version 12, neighbor version 12
  2 accepted prefixes consume 32 bytes

  Prefixes accepted 1 (consume 4 bytes), withdrawn 0 by peer
  Prefixes advertised 0, rejected 0, withdrawn 0 from peer
  Connections established 3; dropped 2
  Last reset 00:00:39, due to Closed by neighbor

  Notification History
    'OPEN error/Bad AS' Sent : 0 Recv: 1

  Local host: 5ffe:10::4, Local port: 179
  Foreign host: 5ffe:10::3, Foreign port: 35470

  Notification History
    'Connection Reset' Sent : 1 Recv: 0

  BGP neighbor is 5ffe:11::3, remote AS 1, external link
    BGP version 4, remote router ID 5.5.5.3
    BGP state ESTABLISHED, in this state for 00:00:28
    Last read 00:00:28, last write 00:00:28
    Hold time is 180, keepalive interval is 60 seconds
    Received 27 messages, 3 notifications, 0 in queue
    Sent 0 messages, 0 notifications, 0 in queue
    Received 8 updates, Sent 0 updates
    Route refresh request: received 0, sent 0
    Minimum time between advertisement runs is 30 seconds
    Minimum time before advertisements start is 0 seconds

  Capabilities received from neighbor for IPv6 Unicast :
    MULTIPROTO_EXT(1)
    ROUTE_REFRESH(2)
    CISCO_ROUTE_REFRESH(128)
    Capabilities advertised to neighbor for IPv6 Unicast :
    MULTIPROTO_EXT(1)
    ROUTE_REFRESH(2)
    CISCO_ROUTE_REFRESH(128)

  For address family: IPv6 Unicast
  BGP table version 12, neighbor version 12
  2 accepted prefixes consume 32 bytes
  Prefix advertised 0, rejected 0, withdrawn 0

  Connections established 3; dropped 2
  Last reset 00:00:41, due to Closed by neighbor

  Notification History
    'OPEN error/Bad AS' Sent : 0 Recv: 1

Local host: 5ffe:11::4, Local port: 179
```

show ip bgp ipv6 unicast peer-group

Allows you to view information on the BGP peers in a peer group.

Syntax

`show ip bgp ipv6 unicast peer-group [peer-group-name [summary]]`

Parameters

peer-group-name	(OPTIONAL) Enter the name of a peer group to view information about that peer group only.
summary	(OPTIONAL) Enter the keyword `summary` to view status information of the peers in that peer group. The output is the same as that found in the `show ip bgp ipv6 unicast summary` command.

Command Modes

- EXEC
- EXEC Privilege

Command History	Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

neighbor peer-group (assigning peers) — assigns a peer to a peer-group.

neighbor peer-group (creating group) — creates a peer group.

show ip bgp ipv6 unicast summary

Allows you to view the status of all BGP connections.

Syntax `show ip bgp ipv6 unicast summary`

Command Modes

- EXEC
- EXEC Privilege

Command History	Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show ip bgp ipv6 unicast summary` command shown in the Example below.

Field	Description
BGP router identifier	Displays the local router ID and the AS number.
BGP table version	Displays the BGP table version and the main routing table version.
network entries	Displays the number of network entries, route paths, and the amount of memory used to process those entries.
BGP path attribute entries	Displays the number of BGP path attributes and the amount of memory used to process them.
BGP AS-PATH entries	Displays the number of BGP AS_PATH attributes processed and the amount of memory used to process them.
BGP community entries	Displays the number of BGP COMMUNITY attributes processed and the amount of memory used to process them. The `show ip bgp ipv6 unicast community` command provides more details on the COMMUNITY attributes.
Dampening enabled	Displayed only when dampening is enabled. Displays the number of paths designated as history, dampened, or penalized.
Neighbor	Displays the BGP neighbor address.

Field	Description
AS	Displays the AS number of the neighbor.
MsgRcvd	Displays the number of BGP messages that neighbor received.
MsgSent	Displays the number of BGP messages that neighbor sent.
TblVer	Displays the version of the BGP table that was sent to that neighbor.
InQ	Displays the number of messages from that neighbor waiting to be processed.
OutQ	Displays the number of messages waiting to be sent to that neighbor. If a number appears in parentheses, the number represents the number of messages waiting to be sent to the peer group.
Up/Down	Displays the amount of time (in hours:minutes:seconds) that the neighbor is in the Established stage. If the neighbor has never moved into the Established stage, the word never is displayed.
State/Pfx	If the neighbor is in Established stage, the number of network prefixes received. If a maximum limit was configured with the `neighbor maximum-prefix` command, (prfxd) appears in this column. If the neighbor is not in Established stage, the current stage is displayed (Idle, Connect, Active, OpenSent, OpenConfirm). When the peer is transitioning between states and clearing the routes received, the phrase (Purging) may appear in this column. If the neighbor is disabled, the phrase (Admin shut) appears in this column.

Example

```
Dell#show ip bgp ipv6 unicast summary
BGP router identifier 5.5.10.4, local AS number 100
BGP table version is 12, main routing table version 12
2 network entrie(s) and 4 paths using 536 bytes of memory
1 BGP path attribute entrie(s) using 112 bytes of memory
1 BGP AS-PATH entrie(s) using 39 bytes of memory
Dampening enabled. 0 history paths, 0 dampened paths, 0
penalized paths

Neighbor   AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/Pfx

5ffe:10::3  1    28     0       12   0     0 00:01:01   2
5ffe:11::3  1    27     0       12   0     0 00:00:55   2
Dell#
```

27

iSCSI Optimization

Internet small computer system interface (iSCSI) optimization enables quality-of-service (QoS) treatment for iSCSI storage traffic.

To configure and verify the iSCSI optimization feature, use the following Dell Networking Operating System (OS) commands.

advertise dcbx-app-tlv

Configure DCBX to send iSCSI TLV advertisements.

Syntax

`advertise dcbx-app-tlv iscsi`

To disable DCBX iSCSI TLV advertisements, use the `no advertise dcbx-app-tlv iscsi` command.

Defaults

Disabled.

Command Modes

PROTOCOL LLDP

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

You can configure iSCSI TLVs to send either globally or on a specified interface. The interface configuration takes priority over global configuration.

iscsi aging time

Set the aging time for iSCSI sessions.

Syntax

`iscsi aging time` *`time`*

To remove the iSCSI session aging time, use the `no iscsi aging time` command.

Parameters

time	Enter the aging time for the iSCSI session. The range is from 5 to 43,200 minutes.

Defaults	**10 minutes**
Command Modes	CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

iscsi cos

Set the QoS policy that is applied to the iSCSI flows.

Syntax

```
iscsi cos {enable | disable | dot1p vlan-priority-value
[remark] | dscp dscp-value [remark]}
```

To disable the QoS policy, use the `no iscsi cos dscp` command.

Parameters

enable	Enter the keyword `enable` to allow the application of preferential QoS treatment to iSCSI traffic so that the iSCSI packets are scheduled in the switch with a dot1p priority 4 regardless of the VLAN priority tag in the packet. The default is: the iSCSI packets are handled with dotp1 priority 4 without remark.
disable	Enter the keyword `disable` to disable the application of preferential QoS treatment to iSCSI frames.
dot1p *vlan-priority-value*	Enter the dot1p value of the VLAN priority tag assigned to the incoming packets in an iSCSI session. The range is from 0 to 7. The default is the dot1p value in ingress iSCSI frames is not changed and is the same priority is used in iSCSI TLV advertisements if you did not enter the `iscsi priority-bits` command.
dscp *dscp-value*	Enter the DSCP value assigned to the incoming packets in an iSCSI session. The valid range is from 0 to 63. The default is: the DSCP value in ingress packets is not changed.
remark	Marks the incoming iSCSI packets with the configured dot1p or DSCP value when they egress to the switch. The default is: the dot1and DSCP values in egress packets are not changed.

Defaults	The default dot1p VLAN priority value is 4 without the `remark` option.
Command Modes	CONFIGURATION

Command History	**Version 9.2(0.0)**	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

iscsi enable

Globally enable iSCSI optimization.

Syntax

`iscsi` *`enable`*

To disable iSCSI optimization, use the `no iscsi enable` command.

Parameters

enable	Enter the keyword `enable` to enable the iSCSI optimization feature.

Defaults Disabled.

Command Modes CONFIGURATION

Command History	**Version 9.2(0.0)**	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

When you enable the iSCSI feature using the `iscsi enable` command, flow control settings are set to `rx on tx off` on all interfaces.

iscsi priority-bits

Configure the priority bitmap that advertises in the iSCSI application TLVs.

Syntax

`iscsi priority-bits`

To remove the configured priority bitmap, use the `no iscsi priority-bits` command.

Defaults **4** (0x10 in the bitmap)

Command Modes PROTOCOL LLDP (only on the global, not on the interface)

Command History	**Version 9.2(0.0)**	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

iscsi profile-compellant

Configure the auto-detection of Dell Compellent arrays on a port.

Syntax `iscsi profile-compellent`

Defaults Dell Compellent disk arrays are not detected.

Command Modes INTERFACE

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

iscsi target port

Configure the iSCSI target ports and optionally, the IP addresses on which iSCSI communication is monitored.

Syntax `iscsi target port [`*`tcp-port-2...tcp-port-16`*`]ip-address [`*`ip-address`*`]`

To remove the configured iSCSI target ports or IP addresses, use the `no iscsi target port` command.

Parameters

tcp-port-2...tcpport - 16	Enter the tcp-port number of the iSCSI target ports. The `tcp-port-n` is the TCP port number or a list of TCP port numbers on which the iSCSI target listens to requests. Separate port numbers with a comma. The default is **860, 3260**.
ip-address	(Optional) Enter the ip-address that the iSCSI monitors. The ip-address specifies the IP address of the iSCSI target.

Defaults **860, 3260**

Command Modes CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

You can configure up to 16 target TCP ports on the switch in one command or multiple commands.

When you use the `no iscsi target port` command and the TCP port you wish to delete is one bound to a specific IP address, the IP address value must be included in the command.

show iscsi

Display the currently configured iSCSI settings.

Syntax

```
show iscsi
```

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show iscsi
iSCSI is enabled
iSCSI session monitoring is disabled
iSCSI COS : dot1p is 4 no-remark
Session aging time: 10
Maximum number of connections is 256
------------------------------------------------
iSCSI Targets and TCP Ports:
------------------------------------------------
TCP Port Target IP Address
3260
860
```

Related Commands

- show iscsi sessions — displays information about active iSCSI sessions on the switch.
- show iscsi sessions detailed — displays detailed information about active iSCSI sessions on the switch.
- show run iscsi — shows `run iscsi`.

show iscsi session

Display information about active iSCSI sessions on the switch.

Syntax `show iscsi session`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell# show isci session
Session 0:
------------------------------------------------------
Target: iqn.2001-05.com.equallogic:
0-8a0906-0e70c2002-10a0018426a48c94-iom010
Initiator: iqn.1991-05.com.microsoft:win-x918v27yajg
ISID: 400001370000

Session 1:
---------------------------------------------------------
Target: iqn.2001-05.com.equallogic:
0-8a0906-0f60c2002-0360018428d48c94-iom011
Initiator: iqn.1991-05.com.microsoft:win-x918v27yajg
ISID: 400001370000.
```

Related Commands

- show iscsi — displays the currently configured iSCSI settings.
- show iscsi sessions detailed — displays detailed information about active iSCSI sessions on the switch.
- show run iscsi — shows `run iscsi`.

show iscsi session detailed

Display detailed information on active iSCSI sessions on the switch.

Syntax `show iscsi session detailed [session` *`isid`*`]`

Parameters

isid	Enter the session's iSCSi ID to display detailed information about the specified iSCSi session.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell# show isci session detailed
Session 0 :
---------------------------------------------------
Target:iqn.2010-11.com.ixia:ixload:iscsi-TG1
Initiator:iqn.2010-11.com.ixia.ixload:initiator-iscsi-2c
Up Time:00:00:01:28(DD:HH:MM:SS)
Time for aging out:00:00:09:34(DD:HH:MM:SS)
ISID:806978696102
Initiator  Initiator Target      Target  Connection
IP Address TCP Port  IP Address  TCPPort ID
10.10.0.44 33345     10.10.0.101 3260    0
Session 1 :
----------------------------------------------------
Target:iqn.2010-11.com.ixia:ixload:iscsi-TG1
Initiator:iqn.2010-11.com.ixia.ixload:initiator-iscsi-35
Up Time:00:00:01:22(DD:HH:MM:SS)
Time for aging out:00:00:09:31(DD:HH:MM:SS)
ISID:806978696102
Initiator  Initiator Target     Target  Connection
IP Address TCP Port  IP Address TCPPort ID
10.10.0.53 33432     10.10.0.101 3260   0
```

Related Commands

- show iscsi — displays the currently configured iSCSI settings.
- show iscsi sessions — displays information about active iSCSI sessions on the switch.
- show run iscsi — shows `run iscsi`.

show run iscsi

Display all globally configured non-default iSCSI settings in the current session.

Syntax

`show run iscsi`

Command Modes

EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

- show iscsi — displays the currently configured iSCSI settings.
- show iscsi sessions — show iscsi session — displays detailed information about active iSCSI sessions on the switch.
- show iscsi sessions detailed — displays detailed information on active iSCSI sessions on the switch.

28

Intermediate System to Intermediate System (IS-IS)

The intermediate system to intermediate system (IS-IS) protocol for IPv4 and IPv6 is supported on the on the MXL 10/40GbE Switch IO Module.

IS-IS is an interior gateway protocol that uses a shortest-path-first algorithm. IS-IS facilitates the communication between open systems, supporting routers passing both IP and OSI traffic.

A router is considered an intermediate system. Networks are partitioned into manageable routing domains, called areas. Intermediate systems send, receive, and forward packets to other routers within their area (Level 1 and Level 1-2 devices). Only Level 1-2 and Level 2 devices communicate with other areas.

IS-IS protocol standards are listed in the Standard Compliance chapter in the *Dell Networking OS Configuration Guide*.

NOTE: The fundamental mechanisms of IS-IS are the same between IPv4 and IPv6. Where there are differences between the two versions, they are identified and clarified in this chapter. Except where identified, the information in this chapter applies to both protocol versions.

adjacency-check

Verify that the “protocols supported” field of the IS-IS neighbor contains matching values to this router.

Syntax	`adjacency-check` To disable adjacency check, use the `no adjacency-check` command.
Defaults	Enabled.
Command Modes	• ROUTER ISIS (*for IPv4*) • CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)
Command History	Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	To perform protocol-support consistency checks on hello packets, use this command. The adjacency-check is enabled by default.

advertise

Leak routes between levels (distribute IP prefixes between Level 1 and Level 2 and vice versa).

Syntax

`advertise {level1-into-level2 | level2-into-level1} prefix-list-name`

To return to the default, use the `no advertise {level1-into-level2 | level2-into-level1}[prefix-list-name]` command.

Parameters

level1-into-level2	Enter the keywords `level1-into-level2` to advertise Level 1 routes into Level 2 LSPs. This setting is the default.
level2-into-level1	Enter the keywords `level2-into-level1` to advertise Level 2 inter-area routes into Level 1 LSPs. This behavior is described in RFC 2966.
prefix-list-name	Enter the name of a configured IP prefix list. Routes meeting the criteria of the IP Prefix list are leaked.

Defaults

level1-into-level2 (Level 1 to Level 2 leaking enabled.)

Command Modes

- ROUTER ISIS (*for IPv4*)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

You cannot disable leaking from one level to another; however, you can regulate the rate flow from one level to another using an IP Prefix list. If you do not configure the IP Prefix list, all routes are leaked.

You can find more information in IETF RFC 2966, *Domain-wide Prefix Distribution with Two-Level IS-IS*.

area-password

Configure a hash message authentication code (HMAC) password for an area.

Syntax

`area-password [hmac-md5 | encryption-type] password`

To delete a password, use the `no area-password` command.

Parameters

hmac-md5	(OPTIONAL) Enter the keywords `hmac-md5` to encrypt the password.
encryption-type	(OPTIONAL) Enter `7` to encrypt the password using DES.

password	Enter a 1 to 16-character length alphanumeric string to prevent unauthorized access or incorrect routing information corrupting the link state database. The password is processed as plain text, which only provides limited security.

Defaults

Not configured.

Command Modes

ROUTER ISIS

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To prevent the link state database from receiving incorrect routing information from unauthorized routers, use the `area-password` command on routers within an area.

The configured password injects into Level 1 LSPs, CSNPs, and PSNPs.

Related Commands

- domain-password — allows you to set the authentication password for a routing domain.
- isis password — allows you to configure an authentication password for an interface.

clear config

Clear IS-IS configurations that display under the *router isis* heading of the `show running-config` command output.

Syntax

`clear config`

Command Modes

ROUTER ISIS

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

CAUTION: Use caution when you enter this command. Back up your configuration prior to using this command or your IS-IS configuration will be erased.

Related Commands

copy — saves the current configuration to another location.

clear isis

Restart the IS-IS process. All IS-IS data is cleared.

Syntax	`clear isis [tag] {* | database | traffic}`
Parameters	

tag	(Optional) Enter an alphanumeric string to specify the IS-IS routing tag area.
*	Enter the keyword `*` to clear all IS-IS information and restart the IS-IS process. This command removes IS-IS neighbor information and IS-IS LSP database information and the full SPF calculation is done.
database	Clears IS-IS LSP database information.
traffic	Clears IS-IS counters.

Command Modes	EXEC Privilege
Command History	

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

clns host

Define a name-to-network service mapping point (NSAP) that you use with commands that require NSAPs and system IDs.

Syntax	`clns host name nsap`
Parameters	

name	Enter an alphanumeric string to identify the name-to-NSAP mapping.
nsap	Enter a specific NSAP address that is associated with the name parameter.

Defaults	Not configured.
Command Modes	ROUTER ISIS
Command History	

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information	To configure a shortcut name that you can use instead of entering a long string of numbers associated with an NSAP address, use this command.
Related Commands	hostname dynamic — enables dynamic learning of host names from routers in the domain and allows the routers to advertise the host names in LSPs.

debug isis

Enable debugging for all IS-IS operations.

Syntax

`debug isis`

To disable debugging of IS-IS, use the `no debug isis` command.

Command Modes

EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Entering `debug isis` enables all debugging parameters.

To display all debugging information in one output, use this command. To turn off debugging, you normally enter separate `no` forms of each command. To disable all debug messages for IS-IS at once, enter the `no debug isis` command.

debug isis adj-packets

Enable debugging on adjacency-related activity such as hello packets that are sent and received on IS-IS adjacencies.

Syntax

`debug isis adj-packets [`*`interface`*`]`

To turn off debugging, use the `no debug isis adj-packets [`*`interface`*`]` command.

Parameters

interface	(OPTIONAL) Identifies the interface type slot/port as one of the following: • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

Command Modes

EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

debug isis local-updates

To debug IS-IS local update packets, enable debugging on a specific interface and provides diagnostic information.

Syntax	`debug isis local-updates [interface]` To turn off debugging, use the `no debug isis local-updates [interface]` command.
Parameters	*interface* — (OPTIONAL) Identifies the interface type slot/port as one of the following: • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.
Command Modes	EXEC Privilege
Command History	Version 9.2(0.0) — Introduced on the MXL 10/40GbE Switch IO Module.

debug isis snp-packets

To debug IS-IS complete sequence number PDU (CSNP) and partial sequence number PDU (PSNP) packets, enable debugging on a specific interface and provides diagnostic information.

Syntax	`debug isis snp-packets [interface]` To turn off debugging, use the `no debug isis snp-packets [interface]` command.
Parameters	*interface* — (OPTIONAL) Identifies the interface type slot/port as one of the following: • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

Command Modes	EXEC Privilege	
Command History	Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

debug isis spf-triggers

Enable debugging on the events that triggered IS-IS shortest path first (SPF) events for debugging purposes.

Syntax

`debug isis spf-triggers`

To turn off debugging, use the `no debug isis spf-triggers` command.

Command Modes	EXEC Privilege	
Command History	Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

debug isis update-packets

Enable debugging on link state PDUs (LSPs) that a router detects.

Syntax

`debug isis update-packets [`*`interface`*`]`

To turn off debugging, use the `no debug isis update-packets [`*`interface`*`]` command.

Parameters

interface	(OPTIONAL) Identifies the interface type slot/port as one of the following: • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

Command Modes	EXEC Privilege	
Command History	Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

default-information originate

Generates a default route into an IS-IS routing domain and controls the distribution of default information.

Syntax `default-information originate [always] [metric metric] [route-map map-name]`

To disable the generation of a default route into the specified IS-IS routing domain, use the `no default-information originate [always] [metric metric] [route-map map-name]` command.

Parameters

always	(OPTIONAL) Enter the keyword `always` to have the default route always advertised.
metric *metric*	(OPTIONAL) Enter the keyword `metric` then a number to assign to the route. The range is from 0 to 16777215.
route-map *map-name*	(OPTIONAL) A default route the routing process generates if the route map is satisfied.

Defaults Not configured.

Command Modes

- ROUTER ISIS (for IPv4)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (for IPv6)

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

When you use this command to redistribute routes into a routing domain, the router becomes an autonomous system (AS) boundary router. An AS boundary router does not always generate a default route into a routing domain. The router still requires its own default route before it can generate one.

How a metric value assigned to a default route advertises depends on the `metric-style` command configuration. If the `metric-style` command is set for Narrow mode and the metric value in the `default-information originate` command is set to a number higher than 63, the metric value advertised in the LSPs is 63. If the `metric-style` command is set for Wide mode, the metric value in the `default-information originate` command is advertised.

Related Commands

- redistribute — redistributes routes from one routing domain to another routing domain.
- isis metric — configures a metric for an interface.
- metric-style — sets the metric style for the router.
- show isis database — displays the IS-IS link state database.

description

Enter a description of the IS-IS routing protocol.

Syntax	`description {description}` To remove the description, use the `no description {description}` command.
Parameters	

description	Enter a description to identify the IS-IS protocol (80 characters maximum).

Defaults	none
Command Modes	ROUTER ISIS
Command History	

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands	router isis — Enter ROUTER mode on the switch.

distance

Define the administrative distance for learned routes.

Syntax	`distance weight [ip-address mask [prefix-list]]` To return to the default values, use the `no distance weight` command.
Parameters	

weight	The administrative distance value indicates the reliability of a routing information source. The range is from 1 to 255. (A higher relative value indicates lower reliability. Routes with smaller values are given preference.) The default is **115**.
ip-address mask	(OPTIONAL) Enter an IP address in dotted decimal format and enter a mask in either dotted decimal or /prefix format.
prefix-list	(OPTIONAL) Enter the name of a prefix list name.

Defaults	weight = **115**
Command Modes	ROUTER ISIS (*for IPv4*) CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)
Command History	

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information	The administrative distance indicates the trust value of incoming packets. A low administrative distance indicates a high trust rate. A high value indicates a lower trust rate. For example, a weight of 255 is interpreted that the routing information source is not trustworthy and should be ignored.

distribute-list in

Filter network prefixes received in updates.

Syntax

`distribute-list prefix-list-name in [interface]`

To return to the default values, use the `no distribute-list prefix-list-name in [interface]` command.

Parameters

prefix-list-name	Specify the prefix list to filter prefixes in routing updates.
interface	(OPTIONAL) Identifies the interface type slot/port as one of the following: • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

Defaults

Not configured.

Command Modes

- ROUTER ISIS (*for IPv4*)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

- distribute-list out — suppresses networks from being advertised in updates.
- redistribute — redistributes routes from one routing domain to another routing domain.

distribute-list out

Suppress network prefixes from being advertised in outbound updates.

Syntax

```
distribute-list prefix-list-name out [connected | bgp as number
| ospf process-id | rip | static]
```

To return to the default values, use the `no distribute-list prefix-list-name out [bgp as number connected | ospf process-id | rip | static]` command.

Parameters

prefix-list-name	Specify the prefix list to filter prefixes in routing updates.
connected	(OPTIONAL) Enter the keyword `connected` for directly connected routing process.
ospf *process-id*	(OPTIONAL) Enter the keyword `ospf` then the OSPF process-ID number. The range is from 1 to 65535.
bgp *as number*	(OPTIONAL) Enter the BGP then the AS Number. The range is from 1 to 65535.
rip	(OPTIONAL) Enter the keyword `rip` for RIP routes.
static	(OPTIONAL) Enter the keyword `static` for user-configured routing process.

Defaults

Not configured.

Command Modes

- ROUTER ISIS (*for IPv4*)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

You can assign a name to a routing process so a prefix list IS applied to only the routes derived from the specified routing process.

Related Commands

- distribute-list in — filters the networks received in updates.
- redistribute — redistributes routes from one routing domain to another routing domain.

distribute-list redistributed-override

Suppress flapping of routes when the same route is redistributed into IS-IS from multiple routers in the network.

Syntax

```
distribute-list redistributed-override in
```

To return to the default, use the `no distribute-list redistributed-override in` command.

Defaults none

Command Modes

- ROUTER ISIS (*for IPv4*)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information When you execute this command, IS-IS does not download the route to the routing table if the same route was redistributed into IS-IS routing protocol on the same router.

domain-password

Set the authentication password for a routing domain.

Syntax `domain-password [hmac-md5 | encryption-type] password`

To disable the password, use the `no domain-password` command.

Parameters

hmac-md5	(OPTIONAL) Enter the keywords `hmac-md5` to encrypt the password using MD5.
encryption-type	(OPTIONAL) Enter `7` to encrypt the password using DES.
password	Enter an alphanumeric string up to 16 characters long. If you do not specify an `encryption type` or `hmac-md5` keywords, the password is processed as plain text which provides limited security.

Defaults No default password.

Command Modes ROUTER ISIS

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information The domain password is inserted in Level 2 link state PDUs (LSPs), complete sequence number PDUs (CSNPs), and partial sequence number PDUs (PSNPs).

Related Commands

- area-password — configures an IS-IS area authentication password.
- isis priority — configures the authentication password for an interface.

graceful-restart ietf

Enable graceful restart on an IS-IS router.

Syntax	`graceful-restart ietf` To return to the default, use the `no graceful-restart ietf` command.
Parameters	**ietf**: Enter `ietf` to enable graceful restart on the IS-IS router.
Defaults	Graceful restart disabled.
Command Modes	ROUTER ISIS
Command History	**Version 9.2(0.0)**: Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	Every graceful restart enabled router's HELLO PDUs includes a restart TLV. This restart enables (re)starting as well as the existing ISIS peers to detect the GR capability of the routers on the connected network. A flag in the Restart TLV contains restart request (RR), restart acknowledge (RA) and suppress adjacency advertisement (SA) bit flags. The ISIS graceful restart-enabled router can co-exist in mixed topologies where some routers are graceful restart-enabled and others are not. For neighbors that are not graceful restart-enabled, the restarting router brings up the adjacency per the usual methods.

graceful-restart interval

Set the graceful restart grace period, the time during that all graceful restart attempts are prevented.

Syntax	`graceful-restart interval` *`minutes`* To return to the default, use the `no graceful-restart interval` command.
Parameters	*minutes*: Enter the graceful-restart interval minutes. The range is from 1 to 20 minutes. The default is **5 minutes**.
Defaults	**5 minutes**
Command Modes	ROUTER ISIS
Command History	**Version 9.2(0.0)**: Introduced on the MXL 10/40GbE Switch IO Module.

graceful-restart t1

Set the graceful restart wait time before unacknowledged restart requests are generated. This wait time is the interval before the system sends a restart request (an IIH with RR bit set in Restart TLV) until the CSNP is received from the helping router.

Syntax

`graceful-restart t1 {interval seconds | retry-times value}`

To return to the default, use the `no graceful-restart t1` command.

Parameters

interval	Enter the keyword `interval` to set the wait time. The range is from 5 to 120 seconds. The default is **5 seconds**.
retry-times	Enter the keywords `retry-times` to set the number of times the request interval is extended until a CSNP is received from the helping router. The range is from 1 to 10 attempts. The default is **1**.

Defaults

Refer to Parameters.

Command Modes

ROUTER ISIS

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

graceful-restart t2

Configure the wait time for the graceful restart timer T2 that a restarting router uses as the wait time for each database to synchronize.

Syntax

`graceful-restart t2 {level-1 | level-2} seconds`

To return to the default, use the `no graceful-restart t2` command.

Parameters

level-1, level-2	Enter the keywords `level-1` or `level-2` to identify the database instance type to which the wait interval applies.
seconds	Enter the `gracefule-restart t2` time in seconds. The range is from 5 to 120 seconds. The default is **30 seconds**.

Defaults

30 seconds

Command Modes

ROUTER ISIS

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

graceful-restart t3

Configure the overall wait time before graceful restart completes.

Syntax

`graceful-restart t3 {adjacency | manual} *seconds*`

To return to the default, use the `no graceful-restart t3` command.

Parameters

adjacency	Enter the keyword `adjacency` so that the restarting router receives the remaining time value from its peer and adjusts its T3 value so if you have configured this option.
manual	Enter the keyword `manual` to specify a time value that the restarting router uses. The range is from 50 to 120 seconds. The default is **30 seconds**.

Defaults

manual, **30 seconds**

Command Modes

ROUTER ISIS

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The running router sets the remaining time value to the current adjacency hold time. You can override this setting by implementing this command.

Override the default restart-wait time by entering the `no graceful-restart restart-wait` command. When you disable `restart-wait`, the current adjacency hold time is used.

Set the t3 timer to `adjacency` on the restarting router when implementing this command. The restarting router gets the remaining time value from its peer and adjusts its T3 value so only when you have configured `graceful-restart t3 adjacency`.

Related Commands

graceful-restart restart-wait — enables the graceful restart maximum wait time before a restarting peer comes up.

graceful-restart restart-wait

Enable the graceful restart maximum wait time before a restarting peer comes up.

Syntax

NOTE: Set the t3 timer to `adjacency` on the restarting router when implementing this command.

`graceful-restart restart-wait *seconds*`

To return to the default, use the `no graceful-restart restart-wait` command.

Parameters

seconds	Enter the graceful restart time in seconds. The range is from 5 to 300 seconds. The default is **30 seconds**.

Defaults

30 seconds

Command Modes

ROUTER ISIS

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

graceful-restart t3 — configures the overall wait time before graceful restart completes.

hello padding

Use to turn ON or OFF padding for LAN and point-to-point hello PDUs or to selectively turn padding ON or OFF for LAN or point-to-point hello PDUs.

Syntax

`hello padding [multi-point | point-to-point]`

To return to the default, use the `no hello padding [multi-point | point-to-point]` command.

Parameters

multi-point	(OPTIONAL) Enter the keywords `multi-point` to pad only LAN hello PDUs.
point-to-point	(OPTIONAL) Enter the keywords `point-to-point` to pad only point-to-point PDUs.

Defaults

Both LAN and point-to-point hello PDUs are padded.

Command Modes

ROUTER ISIS

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

IS-IS hellos are padded to the full maximum transmission unit (MTU) size. Padding IS-IS Hellos (IIHS) to the full MTU provides early error detection of large frame transmission problems or mismatched MTUs on adjacent interfaces.

Related Commands

isis hello padding — turns ON or OFF hello padding on an interface basis.

hostname dynamic

Enables dynamic learning of hostnames from routers in the domain and allows the routers to advertise the hostname in LSPs.

Syntax	`hostname dynamic` To disable this command, use the `no hostname dynamic` command.
Defaults	Enabled.
Command Modes	ROUTER ISIS
Command History	**Version 9.2(0.0)** Turn ON or OFF hello padding on an interface basis.
Usage Information	To build name-to-systemID mapping tables through the protocol, use this command. All `show` commands that display systems also display the hostname.
Related Commands	clns host — defines a name-to-NSAP mapping.

ignore-lsp-errors

Ignore LSPs with bad checksums instead of purging those LSPs.

Syntax	`ignore-lsp-errors` To return to the default values, use the `no ignore-lsp-errors` command.
Defaults	In IS-IS, the default deletes LSPs with internal checksum errors (`no ignore-lsp-errors`).
Command Modes	ROUTER ISIS
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	IS-IS normally purges LSPs with an incorrect data link checksum causing the LSP source to regenerate the message. A cycle of purging and regenerating LSPs can occur when a network link continues to deliver accurate LSPs even though there is a link causing data corruption. This process could cause disruption to your system operation.

ip router isis

Configure IS-IS routing processes on an interface and attach an area tag name to the routing process.

Syntax	`ip router isis [tag]` To disable IS-IS on an interface, use the `no ip router isis [tag]` command.
Parameters	*tag* — (OPTIONAL) The tag you specify identifies a specific area routing process. If you do not specify a tag, a null tag is assigned.
Defaults	No processes are configured.
Command Modes	INTERFACE
Command History	**Version 9.2(0.0)** — Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	To assign a network entity title to enable IS-IS, use the `net` command.
Related Commands	• net — configures an IS-IS network entity title (NET) for the routing process. • router isis — enables the IS-IS routing protocol.

ipv6 router isis

Enable the IPv6 IS-IS routing protocol and specify an IPv6 IS-IS process.

Syntax	`ipv6 router isis [tag]` To disable IS-IS routing, use the `no router isis [tag]` command.
Parameters	*tag* — (OPTIONAL) This parameter is a unique name for a routing process. A null tag is assumed if the tag option is not specified. The tag name must be unique for all IP router processes for a given router.
Defaults	Not configured.
Command Modes	ROUTER ISIS
Command History	**Version 9.2(0.0)** — Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	Configure a network entity title (the `net` command) to specify the area address and the router system ID.

To establish adjacencies and establish dynamic routing, enable routing on one or more interfaces.

You can configure only one IS-IS routing process to perform Level 2 routing. A `level-1-2` designation performs Level 1 and Level 2 routing at the same time.

Related Commands

- net — configures an IS-IS network entity title (NET) for the routing process.
- is-type — assigns a type for a given area.

isis circuit-type

Configure the adjacency type on interfaces.

Syntax

`isis circuit-type {level-1 | level-1-2 | level-2-only}`

To return to the default values, use the `no isis circuit-type` command.

Parameters

level-1	You can form a Level 1 adjacency if there is at least one common area address between this system and neighbors. You cannot form Level 2 adjacencies on this interface.
level-1-2	You can form a Level 1 and Level 2 adjacencies when the neighbor is also configured as Level-1-2 and there is at least one common area, if not, a Level 2 adjacency is established. This setting is the default.
level-2-only	You can form a Level 2 adjacencies when other Level 2 or Level 1-2 routers and their interfaces are configured for Level 1-2 or Level 2. Level 1 adjacencies cannot be established on this interface.

Defaults **level-1-2**

Command Modes INTERFACE

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Because the default establishes Level 1 and Level 2 adjacencies, you do not need to configure this command. Routers in an IS-IS system must be configured as a Level 1-only, Level 1-2, or Level 2-only system.

Only configure interfaces as Level 1 or Level 2 on routers that are between areas (for example, a Level 1-2 router) to prevent the software from sending unused hello packets and wasting bandwidth.

isis csnp-interval

Configure the IS-IS complete sequence number PDU (CSNP) interval on an interface.

Syntax

`isis csnp-interval seconds [level-1 | level-2]`

To return to the default values, use the `no isis csnp-interval [seconds] [level-1 | level-2]` command.

Parameters

seconds	Interval of transmission time between CSNPs on multi-access networks for the designated intermediate system. The range is from 0 to 65535. The default is **10**.
level-1	(OPTIONAL) Independently configures the interval of time between transmission of CSNPs for Level 1.
level-2	(OPTIONAL) Independently configures the interval of time between transmission of CSNPs for Level 2.

Defaults

seconds = **10**; **level-1** (if not otherwise specified)

Command Modes

INTERFACE

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The default values of this command are typically satisfactory transmission times for a specific interface on a designated intermediate system. To maintain database synchronization, the designated routers send CSNPs.

You can configure Level 1 and Level 2 CSNP intervals independently.

isis csnp-interval

Configure the IS-IS complete sequence number PDU (CSNP) interval on an interface.

Syntax

`isis csnp-interval seconds [level-1 | level-2]`

To return to the default values, use the `no isis csnp-interval [seconds] [level-1 | level-2]` command.

Parameters

seconds	Interval of transmission time between CSNPs on multi-access networks for the designated intermediate system. The range is from 0 to 65535. The default is **10**.
level-1	(OPTIONAL) Independently configures the interval of time between transmission of CSNPs for Level 1.
level-2	(OPTIONAL) Independently configures the interval of time between transmission of CSNPs for Level 2.

Defaults	seconds = **10**; **level-1** (if not otherwise specified)
Command Modes	INTERFACE
Command History	Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	The default values of this command are typically satisfactory transmission times for a specific interface on a designated intermediate system. To maintain database synchronization, the designated routers send CSNPs. You can configure Level 1 and Level 2 CSNP intervals independently.

isis hello-multiplier

Specify the number of IS-IS hello packets a neighbor must miss before the router declares the adjacency down.

Syntax

`isis hello-multiplier multiplier [level-1 | level-2]`

To return to the default values, use the `no isis hello-multiplier [multiplier] [level-1 | level-2]` command.

Parameters

multiplier	Specifies an integer that sets the multiplier for the hello holding time. Never configure a hello-multiplier lower than the default (3). The range is from 3 to 1000. The default is **3**.
level-1	(OPTIONAL) Select this value to configure the hello multiplier independently for Level 1 adjacencies. This value is the default.
level-2	(OPTONAL) Select this value to configure the hello multiplier independently for Level 2 adjacencies.

Defaults	multiplier = **3**; **level-1** (if not otherwise specified)
Command Modes	INTERFACE
Command History	Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	The holdtime (the product of the hello-multiplier multiplied by the hello-interval) determines how long a neighbor waits for a hello packet before declaring the neighbor is down so routes can be recalculated.

isis hello padding

Turn ON or OFF padding of hello PDUs from INTERFACE mode.

Syntax	`isis hello padding` To return to the default, use the `no isis hello padding` command.
Defaults	Padding of hello PDUs is enabled (ON).
Command Modes	INTERFACE
Command History	Version 9.2(0.0) — Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	Hello PDUs are “padded” only when both the global and interface padding options are ON. Turning either one OFF disables padding for the corresponding interface.
Related Commands	hello padding — turns ON or OFF padding for LAN and point-to-point hello PDUs.

isis ipv6 metric

Assign metric to an interface for use with IPv6 information.

Syntax

`isis ipv6 metric` *`default-metric`* `[level-1 | level-2]`

To return to the default values, use the `no ipv6 isis metric [`*`default-metric`*`] [level-1 | level-2]` command.

Parameters

default-metric	Metric assigned to the link and used to calculate the cost from each other router via the links in the network to other destinations. You can configure this metric for Level 1 or Level 2 routing. The range is from 0 to 16777215. The default is **10**.
level-1	(OPTIONAL) Enter the keywords `level-1` to configure the shortest path first (SPF) calculation for Level 1 (intra-area) routing. This value is the default.
level-2	(OPTIONAL) Enter the keywords `level-2` to configure the SPF calculation for Level 2 (inter-area) routing.

Defaults	default-metric = **10**; **level-1** (if not otherwise specified)
Command Modes	INTERFACE
Command History	Version 9.2(0.0) — Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information	Dell Networking recommends configuring metrics on all interfaces. Without configuring this command, the IS-IS metrics are similar to hop-count metrics.

isis metric

Assign a metric to an interface.

Syntax

`isis metric default-metric [level-1 | level-2]`

To return to the default values, use the `no isis metric [default-metric] [level-1 | level-2]` command.

Parameters

default-metric	Metric assigned to the link and used to calculate the cost from each other router via the links in the network to other destinations. You can configure this metric for Level 1 or Level 2 routing. The range is from 0 to 63 for narrow and transition metric styles and from 0 to 16777215 for wide metric styles. The default is **10**.
level-1	(OPTIONAL) Enter the keywords `level-1` to configure the shortest path first (SPF) calculation for Level 1 (intra-area) routing. This setting is the default.
level-2	(OPTIONAL) Enter the keywords `level-2` to configure the SPF calculation for Level 2 (inter-area) routing.

Defaults

default-metric = **10**; **level-1** (if not otherwise specified)

Command Modes

INTERFACE

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Dell Networking recommends configuring metrics on all interfaces. Without configuring this command, the IS-IS metrics are similar to hop-count metrics.

isis network point-to-point

Enable the software to treat a broadcast interface as a point-to-point interface.

Syntax

`isis network point-to-point`

To disable the feature, use the `no isis network point-to-point` command.

Defaults	Not enabled.
Command Modes	INTERFACE
Command History	Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

isis password

Configure an authentication password for an interface.

Syntax `isis password [hmac-md5] password [level-1 | level-2]`

To delete a password, use the `no isis password [password] [level-1 | level-2]` command.

Parameters

encryption-type	(OPTIONAL) Enter `7` to encrypt the password using DES.
hmac-md5	(OPTIONAL) Enter the keywords `hmac-md5` to encrypt the password using MD5.
password	Assign the interface authentication password.
level-1	(OPTIONAL) Independently configures the authentication password for Level 1. The router acts as a station router for Level 1 routing. This setting is the default.
level-2	(OPTIONAL) Independently configures the authentication password for Level 2. The router acts as an area router for Level 2 routing.

Defaults	No default password. **level-1** (if not otherwise specified).
Command Modes	INTERFACE
Command History	Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To protect your network from unauthorized access, use this command to prevent unauthorized routers from forming adjacencies.

You can assign different passwords for different routing levels by using the keywords `level-1` and `level-2`.

The `no` form of this command disables the password for Level 1 or Level 2 routing, using the respective keywords `level-1` or `level-2`.

This password provides limited security as it is processed as plain text.

isis priority

Set the priority of the designated router you select.

Syntax	`isis priority value [level-1 | level-2]` To return to the default values, use the `no isis priority [value] [level-1 | level-2]` command.
Parameters	*value* — This value sets the router priority. The higher the value, the higher the priority. The range is from 0 to 127. The default is **64**. level-1 — (OPTIONAL) Specify the priority for Level 1. This setting is the default. level-2 — (OPTIONAL) Specify the priority for Level 2.
Defaults	value = **64**; **level-1** (if not otherwise specified).
Command Modes	INTERFACE
Command History	Version 9.2(0.0) — Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	You can configure priorities independently for Level 1 and Level 2. Priorities determine which router on a LAN is the designated router. Priorities are advertised within hellos. The router with the highest priority becomes the designated intermediate system (DIS). NOTE: Routers with a priority of 0 cannot be a designated router. Setting the priority to 0 lowers the chance of this system becoming the DIS, but does not prevent it. If all the routers have priority 0, one with highest MAC address becomes DIS even though its priority is 0.

is-type

Configure IS-IS operating level for a router.

Syntax	`is-type {level-1 | level-1-2 | level-2-only}` To return to the default values, use the `no is-type` command.

Parameters		
	level-1	Allows a router to act as a Level 1 router.
	level-1-2	Allows a router to act as both a Level 1 and Level 2 router. This setting is the default.
	level-2-only	Allows a router to act as a Level 2 router.

Defaults **level-1-2**

Command Modes ROUTER ISIS

Command History		
	Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The IS-IS protocol automatically determines area boundaries and are able to keep Level 1 and Level 2 routing separate. Poorly planned use of this feature may cause configuration errors, such as accidental area partitioning.

If you are configuring only one area in your network, you do not need to run both Level 1 and Level 2 routing algorithms. You can configure the IS type as Level 1.

log-adjacency-changes

Generate a log messages for adjacency state changes.

Syntax

```
log-adjacency-changes
```

To disable this function, use the `no log-adjacency-changes` command.

Defaults Adjacency changes are not logged.

Command Modes ROUTER ISIS

Command History		
	Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

This command allows you to monitor adjacency state changes, which are useful when you monitor large networks. Messages are logged in the system’s error message facility.

lsp-gen-interval

Set the minimum interval between successive generations of link-state packets (LSPs).

Syntax

```
lsp-gen-interval [level-1 | level-2] interval seconds
[initial_wait_interval seconds [second_wait_interval seconds]]
```

To restore default values, use the `no lsp-gen-interval [level-l | level-2] interval seconds [initial_wait_interval seconds [second_wait_interval seconds]]` command.

Parameters

level-l	(OPTIONAL) Enter the keywords `level-1` to apply the configuration to generation of Level-1 LSPs.
level-2	(OPTIONAL) Enter the keywords `level-2` to apply the configuration to generation of Level-2 LSPs.
interval seconds	Enter the maximum number of seconds between LSP generations. The range is from 0 to 120 seconds. The default is **5 seconds**.
initial_wait_interval seconds	(OPTIONAL) Enter the initial wait time, in seconds, before running the first LSP generation. The range is from 0 to 120 seconds. The default is **1 second**.
second_wait_interval seconds	(OPTIONAL) Enter the wait interval, in seconds, between the first and second LSP generation. The range is from 0 to 120 seconds. The default is **5 seconds**.

Defaults

Refer to *Parameters*.

Command Modes

ROUTER ISIS

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

LSP throttling slows down the frequency at which LSPs are generated during network instability. Even though throttling LSP generations slows down network convergence, no throttling can result in a network not functioning as expected. If network topology is unstable, throttling slows down the scheduling of LSP generations until the topology regains its stability.

The first generation is controlled by the initial wait interval and the second generation is controlled by the second wait interval. Each subsequent wait interval is twice as long as the previous one until the wait interval reaches the maximum wait time specified (`interval seconds`). After the network calms down and there are no triggers for two times the maximum interval, fast behavior is restored (the initial wait time).

lsp-mtu

Set the maximum transmission unit (MTU) of IS-IS link-state packets (LSPs). This command only limits the size of LSPs this router generates.

Syntax

`lsp-mtu size`

To return to the default values, use the `no lsp-mtu` command.

Parameters

size	The maximum LSP size, in bytes. The range is from 128 to 1497 for Non-Jumbo mode and from 128 to 9195 for Jumbo mode. The default is **1497**.

Defaults **1497** bytes.

Command Modes ROUTER ISIS

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information The link MTU and the LSP MTU size must be the same.

Because each device can generate a maximum of 255 LSPs, consider carefully whether you use the `lsp-mtu` command.

lsp-refresh-interval

Set the link state PDU (LSP) refresh interval. LSPs must be refreshed before they expire. When the LSPs are not refreshed after a refresh interval, they are kept in a database until their `max-lsp-lifetime` reaches zero and then LSPs is purged.

Syntax `lsp-refresh-interval` *`seconds`*

To restore the default refresh interval, use the `no lsp-refresh-interval` command.

Parameters

seconds	The LSP refresh interval, in seconds. This value has to be less than the seconds value specified with the `max-lsp-lifetime` command. The range is from 1 to 65535 seconds. The default is **900**.

Defaults **900** seconds

Command Modes ROUTER ISIS

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information The refresh interval determines the rate at which route topology information is transmitted preventing the information from becoming obsolete.

The refresh interval must be less than the LSP lifetime specified with the `max-lsp-lifetime` command. A low value reduces the amount of time that undetected link

	state database corruption can persist at the cost of increased link utilization. A higher value reduces the link utilization the flooding of refreshed packets causes.
Related Commands	max-lsp-lifetime — sets the maximum interval that LSPs persist without being refreshed.

max-area-addresses

Configure manual area addresses.

Syntax

`max-area-addresses number`

To return to the default values, use the `no max-area-addresses` command.

Parameters

number	Set the maximum number of manual area addresses. The range is from 3 to 6. The default is **3**.

Defaults: **3** addresses

Command Modes: ROUTER ISIS

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To configure the number of area addresses on router, use this command. This value must be consistent with routers in the same area, otherwise the router forms only Level 2 adjacencies. The value must be same among all the routers to form Level 1 adjacencies.

max-lsp-lifetime

Set the maximum time that link-state packets (LSPs) exist without being refreshed.

Syntax

`max-lsp-lifetime seconds`

To restore the default time, use the `no max-lsp-lifetime` command.

Parameters

seconds	The maximum lifetime of LSP in seconds. This value must be greater than the `lsp-refresh-interval` command. The higher the value the longer the LSPs are kept. The range is from 1 to 65535. The default is **1200**.

Defaults: **1200** seconds

Command Modes	ROUTER ISIS
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	Change the maximum LSP lifetime with this command. The maximum LSP lifetime must always be greater than the LSP refresh interval. The `seconds` parameter enables the router to keep LSPs for the specified length of time. If the value is higher, the overhead is reduced on slower-speed links.
Related Commands	lsp-refresh-interval — sets the link-state packet (LSP) refresh interval.

maximum-paths

Allows you to configure the maximum number of equal cost paths allowed in a routing table.

Syntax

`maximum-paths number`

To return to the default values, use the `no maximum-paths` command.

Parameters

number	Enter a number as the maximum number of parallel paths an IP routing installs in a routing table. The range is from 1 to 16. The default is **4**.

Defaults **4**

Command Modes

- ROUTER ISIS (*for IPv4*)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

metric-style

To generate and accept old-style, new-style, or both styles of type, length, and values (TLV), configure a router.

Syntax

`metric-style {narrow [transition] | transition | wide [transition]} [level-1 | level-2]`

To return to the default values, use the `no metric-style {narrow [transition] | transition | wide [transition]} [level-1 | level-2]` command.

Parameters

narrow	Allows you to generate and accept old-style TLVs. The metric range is from 0 to 63.
transition	Allows you to generate both old-style and new-style TLVs. The metric range is from 0 to 63.
wide	Allows you to generate and accept only new-style TLVs. The metric range is from 0 to 16777215.
level-1	Enables the metric style on Level 1.
level-2	Enables the metric style on Level 2.

Defaults: **narrow**; if no Level is specified, Level-1 and Level-2 are configured.

Command Modes: ROUTER ISIS

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

If you enter the `metric-style wide` command, the system generates and accepts only new-style TLVs. The router uses less memory and other resources rather than generating both old-style and new-style TLVs.

The new-style TLVs have wider metric fields than old-style TLVs.

Related Commands: isis metric — configures a metric for an interface.

multi-topology

Enables multi-topology IS-IS. It also allows enabling/disabling of old and new style TLVs for IP prefix information in the LSPs.

Syntax

```
multi-topology [transition]
```

To return to a single topology configuration, use the `no multi-topology [transition]` command.

Defaults: Disabled

Command Modes: CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

net

To configure an IS-IS network entity title (NET) for a routing process, use this mandatory command. If you did not configure a NET, the IS-IS process does not start.

Syntax	`net` *`network-entity-title`* To remove a net, use the `no net` *`network-entity-title`* command.

Parameters

network-entity-title	Specify the area address and system ID for an IS-IS routing process. The first 1 to 13 bytes identify the area address. The next 6 bytes identify the system ID. The last 1 byte is the selector byte, always identified as zero zero (00). This argument can be applied to an address or a name.

Defaults	Not configured.
Command Modes	ROUTER ISIS

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

passive-interface

Suppress routing updates on an interface. This command stops the router from sending updates on that interface.

Syntax	`passive-interface` *`interface`* To delete a passive interface configuration, use the `no passive-interface` *`interface`* command.

Parameters

interface	Enter the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the slot/port information. • For Loopback interface, enter the keyword `loopback` then a number from 0 to 16383. • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a SONET interface, enter the keyword `sonet` then the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

Defaults

Not configured.

Command Modes

ROUTER ISIS

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Although the passive interface does not send nor receive routing updates, the network on that interface is still included in the IS-IS updates sent using other interfaces.

redistribute

Redistribute routes from one routing domain to another routing domain.

Syntax

```
redistribute {static | connected | rip} [level-1 | level-1-2 |
level-2] [metric metric-value] [metric-type {external |
internal}] [route-map map-name]
```

To end redistribution or disable any of the specified keywords, use the `no redistribute {static | connected | rip} [metric metric-value] [metric-type {external | internal}] [level-1 | level-1-2 | level-2] [route-map map-name]` command.

Parameters

connected	Enter the keyword `connected` to redistribute active routes into IS-IS.
rip	Enter the keyword `rip` to redistribute RIP routes into IS-IS.
static	Enter the keyword `static` to redistribute user-configured routes into IS-IS.
metric *metric-value*	(OPTIONAL) Assign a value to the redistributed route. The range is from 0 to 16777215. The default is **0**. Use a value that is consistent with the destination protocol.
metric-type {external | internal}	(OPTIONAL) The external link type associated with the default route advertised into a routing domain. Specify one of the following: • `external` • `internal`
level-1	(OPTIONAL) Routes are independently redistributed into IS-IS as Level 1 routes.
level-1-2	(OPTIONAL) Routes are independently redistributed into IS-IS as Level-1-2 routes.
level-2	(OPTIONAL) Routes are independently redistributed into IS-IS as Level 2 routes. This setting is the default.

route-map *map-name*	(OPTIONAL) If you do not enter the route-map argument, all routes are redistributed. If a map-name value is not specified, no routers are imported.

Defaults

- metric metric-value = **0**
- metric-type= internal; **level-2**

Command Modes

- ROUTER ISIS (*for IPv4*)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To redistribute a default route (0.0.0.0/0), configure the `default-information originate` command.

Changing or disabling a keyword in this command does not affect the state of the other command keywords.

When an LSP with an internal metric is received, the system considers the route cost while considering the advertised cost to reach the destination.

Redistributed routing information is filtered with the `distribute-list out` command to ensure that the routes are properly are passed to the receiving routing protocol.

How a metric value assigned to a redistributed route is advertised depends on how on the configuration of the `metric-style` command. If the `metric-style` command is set for Narrow or Transition mode and the metric value in the `redistribute` command is set to a number higher than 63, the metric value advertised in LSPs is 63. If the `metric-style` command is set for Wide mode, the metric value in the `redistribute` command is advertised.

Related Commands

- default-information originate — generates a default route for the IS-IS domain.
- distribute-list out — suppresses networks from being advertised in updates. This command filters redistributed routing information.

redistribute bgp

Redistribute routing information from a BGP process. (New command in Release 6.3.1.)

Syntax

```
redistribute bgp AS number [level-1| level-1-2 | level-2]
[metric metric-value] [metric-type {external| internal}]
[route-map map-name]
```

To return to the default values, use the `no redistribute bgp` command with the appropriate parameters.

Parameters

AS number	Enter a number that corresponds to the autonomous system number. The range is from 1 to 65355.
level-1	(OPTIONAL) Routes are independently redistributed into IS-IS Level 1 routes only.
level-1-2	(OPTIONAL) Routes are independently redistributed into IS-IS Level 1 and Level 2 routes.
level-2	(OPTIONAL) Routes are independently redistributed into IS-IS as Level 2 routes only. This setting is the default.
metric *metric-value*	(OPTIONAL) The value used for the redistributed route. Use a metric value that is consistent with the destination protocol. The range is from 0 to 16777215. The default is **0**.
metric-type {external| internal}	(OPTIONAL) The external link type associated with the default route advertised into a routing domain. The two options are: • `external` • `internal`
route-map *map-name*	`map-name` is an identifier for a configured route map. The route map filters imported routes from the source routing protocol to the current routing protocol. If you do not specify a map-name, all routes are redistributed. If you specify a keyword, but fail to list route map tags, no routes are imported.

Defaults

IS-IS Level 2 routes only

Command Modes

- ROUTER ISIS (*for IPv4*)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

BGP to IS-IS redistribution supports “match” options using route maps. You can set the metric value, level, and metric-type of redistributed routes by the redistribution command. You can “set” more advanced options using route maps.

Example

```
Dell(conf)#router is
Dell(conf-router_isis)#redistribute bgp 1 level-1 metric 32
metric-type
external route-map rmap-isis-to-bgp
Dell(conf-router_bgp)#show running-config isis
!
router isis
redistribute bgp 1 level-1 metric 32 metric-type external
```

```
route-map
rmap-isis-to-bgp
```

redistribute ospf

Redistribute routing information from an OSPF process.

Syntax

`redistribute ospf process-id [level-1| level-1-2 | level-2] [match {internal | external}] [metric metric-value] [metric-type {external | internal}] [route-map map-name]`

To return to the default values, use the `no redistribute ospf process-id [level-1| level-1-2 | level-2] [match {internal | external}] [metric metric-value][metric-type {external | internal}] [route-map map-name]` command.

Parameters

process-id	Enter a number that corresponds to the OSPF process ID to be redistributed. The range is from 1 to 65355.
metric *metric-value*	(OPTIONAL) The value used for the redistributed route. Use a metric value that is consistent with the destination protocol. The range is from 0 to 16777215. The default is **0**.
metric-type {external | internal}	(OPTIONAL) The external link type associated with the default route advertised into a routing domain. The two options are: • `external` • `internal`
level-1	(OPTIONAL) Routes are independently redistributed into IS-IS as Level 1 routes.
level-1-2	(OPTIONAL) Routes are independently redistributed into IS-IS as Level-1-2 routes.
level-2	(OPTIONAL) Routes are independently redistributed into IS-IS as Level 2 routes. This setting is the default.
match {external | internal}	(OPTIONAL) The command used for OSPF to route and redistribute into other routing domains. The values are • `internal` • `external`
route-map *map-name*	`map-name` is an identifier for a configured route map. The route map should filter imported routes from the source routing protocol to the current routing protocol.

If you do not specify a map-name, all routes are redistributed. If you specify a keyword, but fail to list route map tags, no routes are imported.

Defaults	Refer to Parameters.
Command Modes	• ROUTER ISIS (*for IPv4*) • CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)
Command History	Version 9.2(0.0) — Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	How a metric value assigned to a redistributed route is advertised depends on how on the configuration of the `metric-style` command. If the `metric-style` command is set for Narrow mode and the metric value in the `redistribute ospf` command is set to a number higher than 63, the metric value advertised in LSPs is 63. If the `metric-style` command is set for wide mode, the metric value in the `redistribute ospf` command is advertised.

router isis

Allows you to enable the IS-IS routing protocol and to specify an IP IS-IS process.

Syntax

`router isis [tag]`

To disable IS-IS routing, use the `no router isis [tag]` command.

Parameters

tag	(OPTIONAL) This is a unique name for a routing process. A null tag is assumed if the `tag` option is not specified. The tag name must be unique for all IP router processes for a given router.

Defaults	Not configured.
Command Modes	ROUTER ISIS
Command History	Version 9.2(0.0) — Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Configure a network entity title (the `net` command) to specify the area address and the router system ID.

Enable routing on one or more interfaces to establish adjacencies and establish dynamic routing.

You can configure only one IS-IS routing process to perform Level 2 routing. A `level-1-2` designation performs Level 1 and Level 2 routing at the same time.

Related Commands

- ip router isis — configures IS-IS routing processes for IP on interfaces and attaches an area designator to the routing process.
- net — configures an IS-IS network entity title (NET) for a routing process.
- is-type — assigns a type for a given area.

set-overload-bit

To set the overload bit in its non-pseudonode LSPs, configure the router. This setting prevents other routers from using it as an intermediate hop in their shortest path first (SPF) calculations.

Syntax

`set-overload-bit`

To return to the default values, use the `no set-overload-bit` command.

Defaults

Not set.

Command Modes

- ROUTER ISIS (*for IPv4*)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Set the overload bit when a router experiences problems, such as a memory shortage due to an incomplete link state database which can result in an incomplete or inaccurate routing table. If you set the overload bit in its LSPs, other routers ignore the unreliable router in their SPF calculations until the router has recovered.

show config

Display the changes you made to the IS-IS configuration. Default values are not shown.

Syntax

`show config`

Command Modes

- ROUTER ISIS (*for IPv4*)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Example (Router-Isis)

The bold section identifies that Multi-Topology IS-IS is enabled in Transition mode.

```
Dell(conf-router_isis)#show config
!
router isis
```

```
clns host ISIS 49.0000.0001.F100.E120.0013.00
log-adjacency-changes
net 49.0000.0001.F100.E120.0013.00
!
address-family ipv6 unicast
maximum-paths 16
multi-topology transition
set-overload-bit
spf-interval level-1 100 15 20
spf-interval level-2 120 20 25
exit-address-family
```

Example (Address-Family_IPv6)

The bold section identifies that Multi-Topology IS-IS is enabled in Transition mode.

```
Dell(conf-router_isis-af_ipv6)#show conf
!
address-family ipv6 unicast
maximum-paths 16
multi-topology transition
set-overload-bit
spf-interval level-1 100 15 20
spf-interval level-2 120 20 25
exit-address-family
```

show isis database

Display the IS-IS link state database.

Syntax

`show isis database [level-1 | level-2] [local] [detail | summary] [lspid]`

Parameters

level-1	(OPTIONAL) Displays the Level 1 IS-IS link-state database.
level-2	(OPTIONAL) Displays the Level 2 IS-IS link-state database.
local	(OPTIONAL) Displays local link-state database information.
detail	(OPTIONAL) Detailed link-state database information of each LSP displays when specified. If not specified, a summary displays.
summary	(OPTIONAL) Summary of link-state database information displays when specified.
lspid	(OPTIONAL) Display only the specified LSP.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show isis database` command shown in the following example.

Field	Description
IS-IS Level-1/ Level-2 Link State Database	Displays the IS-IS link state database for Level 1 or Level 2.
LSPID	Displays the LSP identifier. The first six octets are the System ID of the originating router. The first six octets are the System ID of the originating router. The next octet is the pseudonode ID. If this byte is not zero, the LSP describes system links. If this byte is zero (0), the LSP describes the state of the originating router. The designated router for a LAN creates and floods a pseudonode LSP and describes the attached systems. The last octet is the LSP number. An LSP is divided into multiple LSP fragments if there is more data than cannot fit in a single LSP. Each fragment has a unique LSP number. An * after the LSPID indicates that the system originates an LSP where this command was issued.
LSP Seq Num	This value is the sequence number for the LSP that allows other systems to determine if they have received the latest information from the source.
LSP Checksum	This is the checksum of the entire LSP packet.
LSP Holdtime	This value is the amount of time, in seconds, that the LSP remains valid. A zero holdtime indicates that this is a purged LSP and is being removed from the link state database. A value between brackets indicates the duration that the purged LSP stays in the database before being removed.
ATT	This value represents the Attach bit. This value indicates that the router is a Level 2 router and can reach other areas. Level 1-only routers and Level 1-2 routers that have lost connection to other Level 2 routers use the Attach bit to find the closest Level 2 router. They point a default route to the closest Level 2 router.
P	This value represents the P bit. This bit is always set to zero as Dell Networking does not support area partition repair.
OL	This value represents the overload bit, determining congestion. If the overload bit is set, other routers do not use this system as a transit router when calculating routes.

Example

The bold sections identify that MultiTopology IS-IS is enabled.

```
Dell#show isis database

IS-IS Level-1 Link State Database
LSPID    LSP Seq Num LSP Checksum LSP Holdtime ATT/P/OL
ISIS.00-00 * 0x00000006 0xCF43    580          0/0/0

IS-IS Level-2 Link State Database
LSPID    LSP Seq Num LSP Checksum LSP Holdtime ATT/P/OL
ISIS.00-00 * 0x00000006 0xCF43    580          0/0/0
!
Dell#show isis database detail ISIS.00-00

IS-IS Level-1 Link State Database
LSPID    LSP Seq Num LSP Checksum LSP Holdtime ATT/P/OL
ISIS.00-00 * 0x0000002B 0x853B    1075         0/0/0
  Area Address: 49.0000.0001
  NLPID: 0xCC 0x8E
  IP Address: 10.1.1.1
  IPv6 Address: 1011::1
  Topology: IPv4 (0x00) IPv6 (0x8002)
  Metric: 10      IS OSPF.00
  Metric: 10   IS (MT-IPv6) OSPF.00
  Metric: 10      IP 15.1.1.0 255.255.255.0
  Metric: 10   IPv6 (MT-IPv6) 1511::/64
 Metric: 10     IPv6 (MT-IPv6) 2511::/64
 Metric: 10     IPv6 (MT-IPv6) 1011::/64
  Metric: 10      IPv6 1511::/64
  Metric: 10      IP 10.1.1.0 255.255.255.0
    Hostname: ISIS

IS-IS Level-2 Link State Database
LSPID    LSP Seq Num LSP Checksum LSP Holdtime ATT/P/OL
ISIS.00-00 * 0x0000002D 0xB2CD    1075         0/0/0
  Area Address: 49.0000.0001
  NLPID: 0xCC 0x8E
  IP Address: 10.1.1.1
  IPv6 Address: 1011::1
  Topology: IPv4 (0x00) IPv6 (0x8002)
  Metric: 10      IS OSPF.00
 Metric: 10   IS (MT-IPv6) OSPF.00
  Metric: 10      IP 10.1.1.0 255.255.255.0
  Metric: 10      IP 15.1.1.0 255.255.255.0
  Metric: 20      IP 10.3.3.0 255.255.255.0
  Metric: 10   IPv6 (MT-IPv6) 1011::/64
 Metric: 10     IPv6 (MT-IPv6) 1511::/64
 Metric: 10     IPv6 (MT-IPv6) 2511::/64
 Metric: 20     IPv6 (MT-IPv6) 1033::/64
  Metric: 10      IPv6 2511::/64
  Metric: 20      IPv6 1033::/64
  Hostname: ISIS
Dell#
```

show isis graceful-restart detail

Display detailed IS-IS graceful restart related settings.

Syntax `show isis graceful-restart detail`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show isis graceful-restart detail
Configured Timer Value
======================
Graceful Restart    : Enabled
T3 Timer            : Manual
T3 Timeout Value    : 30
T2 Timeout Value    : 30 (level-1), 30 (level-2)
T1 Timeout Value    : 5, retry count: 1
Adjacency wait time : 30

Operational Timer Value
======================
Current Mode/State     : Normal/RUNNING
T3 Time left           : 0
T2 Time left           : 0 (level-1), 0 (level-2)
Restart ACK rcv count  : 0 (level-1), 0 (level-2)
Restart Req rcv count  : 0 (level-1), 0 (level-2)
Suppress Adj rcv count : 0 (level-1), 0 (level-2)
Restart CSNP rcv count : 0 (level-1), 0 (level-2)
Database Sync count    : 0 (level-1), 0 (level-2)
Dell#
```

show isis hostname

Display IS-IS host names configured or learned on the system.

Syntax `show isis hostname`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show isis hostname
System Id       Dynamic Name Static Name
*F100.E120.0013 Force10      ISIS
Dell#
```

show isis interface

Display detailed IS-IS interface status and configuration information.

Syntax

```
show isis interface [interface]
```

Parameters

interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For Loopback interface, enter the keyword `loopback` then a number from 0 to 16383. • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell>show isis int
GigabitEthernet 0/7 is up, line protocol is up
  MTU 1497, Encapsulation SAP
  Routing Protocol: IS-IS
    Circuit Type: Level-1-2
    Interface Index 37847070, Local circuit ID 1
    Level-1 Metric: 10, Priority: 64, Circuit ID: systest-3.01
     Hello Interval: 10, Hello Multiplier: 3, CSNP Interval: 10
    Number of active level-1 adjacencies: 1
    Level-2 Metric: 10, Priority: 64, Circuit ID: systest-3.01
     Hello Interval: 10, Hello Multiplier: 3, CSNP Interval: 10
    Number of active level-2 adjacencies: 1
    Next IS-IS LAN Level-1 Hello in 2 seconds
    Next IS-IS LAN Level-2 Hello in 1 seconds
    LSP Interval: 33
GigabitEthernet 0/8 is up, line protocol is up
  MTU 1497, Encapsulation SAP
  Routing Protocol: IS-IS
    Circuit Type: Level-1-2
    Interface Index 38371358, Local circuit ID 2
    Level-1 Metric: 10, Priority: 64, Circuit ID: systest-3.02
     Hello Interval: 10, Hello Multiplier: 3, CSNP Interval: 10
    Number of active level-1 adjacencies: 1
    Level-2 Metric: 10, Priority: 64, Circuit ID: systest-3.02
     Hello Interval: 10, Hello Multiplier: 3, CSNP Interval: 10
--More--
```

show isis neighbors

Display information about neighboring (adjacent) routers.

Syntax

```
show isis neighbors [level-1 | level-2] [detail] [interface]
```

Parameters

level-1	(OPTIONAL) Displays information about Level 1 IS-IS neighbors.
level-2	(OPTIONAL) Displays information about Level 2 IS-IS neighbors.
detail	(OPTIONAL) Displays detailed information about neighbors.
interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Use this command to confirm that the neighbor adjacencies are operating correctly. If you suspect that they are not, you can verify the specified area addresses of the routers by using the `show isis neighbors` command.

The following describes the `show isis neighbors` command shown in the following example.

Field	Description
System Id	The value that identifies a system in an area.
Interface	The interface, slot, and port in which the router was discovered.
State	The value providing status about the adjacency state. The range is Up and Init.
Type	This value displays the adjacency type (Layer 2, Layer 2 or both).
Priority	IS-IS priority the neighbor advertises. The neighbor with highest priority becomes the designated router for the interface.

Field	Description
Uptime	Displays the interfaces uptime.
Circuit Id	The neighbor's interpretation of the designated router for the interface.

Example

The bold sections below identify that Multi-Topology IS-IS is enabled.

```
Dell#show isis neighbors
System Id Interface State Type Priority Uptime Circuit Id
TEST Gi 7/1 Up L1L2(M) 127 09:28:01 TEST.02
!
Dell#show isis neighbors detail
System Id Interface State Type Priority Uptime Circuit Id
TEST Gi 7/1 Up L1L2(M) 127 09:28:04 TEST.02 Area Address(es):
49.0000.0001
  IP Address(es): 25.1.1.3*
  MAC Address: 0000.0000.0000
  Hold Time: 28
  Link Local Address: fe80::201:e8ff:fe00:492c
  Topology: IPv4 IPv6 , Common (IPv4 IPv6 )
 Adjacency being used for MTs: IPv4 IPv6
Dell#
```

show isis protocol

Display IS-IS routing information.

Syntax `show isis protocol`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Example

The bold section identifies that Multi-Topology IS-IS is enabled.

```
Dell#show isis protocol
IS-IS Router: <Null Tag>
  System Id: F100.E120.0013 IS-Type: level-1-2
  Manual area address(es):
   49.0000.0001
  Routing for area address(es):
   49.0000.0001
  Interfaces supported by IS-IS:
  GigabitEthernet 1/0 - IP - IPv6
  GigabitEthernet 1/1 - IP - IPv6
  GigabitEthernet 1/10 - IP - IPv6
  Loopback 0 - IP - IPv6
Redistributing:
Distance: 115
Generate narrow metrics: level-1-2
Accept narrow metrics:   level-1-2
```

```
Generate wide metrics:   none
Accept wide metrics:     none
Multi Topology Routing is enabled in transition mode.
Dell#
```

show isis traffic

This command allows you to display IS-IS traffic interface information.

Syntax `show isis traffic [interface]`

Parameters

interface	(OPTIONAL) Identifies the interface type slot/port as one of the following: • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show isis traffic` command shown in the following example.

Item	Description
Level-1/Level-2 Hellos (sent/rcvd)	Displays the number of Hello packets sent and received.
PTP Hellos (sent/rcvd)	Displays the number of point-to-point Hellos sent and received.
Level-1/Level-2 LSPs sourced (new/refresh)	Displays the number of new and refreshed LSPs.
Level-1/Level-2 LSPs flooded (sent/rcvd)	Displays the number of flooded LSPs sent and received.
Level-1/Level-2 LSPs CSNPs (sent/rcvd)	Displays the number of CSNP LSPs sent and received.

Item	Description
Level-1/Level-2 LSPs PSNPs (sent/ rcvd)	Displays the number of PSNP LPSs sent and received.
Level-1/Level-2 DR Elections	Displays the number of times designated router elections ran.
Level-1/Level-2 SPF Calculations	Displays the number of shortest path first calculations.
LSP checksum errors received	Displays the number of checksum errors LSPs received.
LSP authentication failures	Displays the number of LSP authentication failures.

Example

```
Dell#sho is traffic
  IS-IS: Level-1 Hellos (sent/rcvd) : 0/721
  IS-IS: Level-2 Hellos (sent/rcvd) : 900/943
  IS-IS: PTP Hellos (sent/rcvd) : 0/0
  IS-IS: Level-1 LSPs sourced (new/refresh) : 0/0
  IS-IS: Level-2 LSPs sourced (new/refresh) : 1/3
  IS-IS: Level-1 LSPs flooded (sent/rcvd) : 0/0
  IS-IS: Level-2 LSPs flooded (sent/rcvd) : 5934/5217
  IS-IS: Level-1 LSPs CSNPs (sent/rcvd) : 0/0
  IS-IS: Level-2 LSPs CSNPs (sent/rcvd) : 472/238
  IS-IS: Level-1 LSPs PSNPs (sent/rcvd) : 0/0
  IS-IS: Level-2 LSPs PSNPs (sent/rcvd) : 10/337
  IS-IS: Level-1 DR Elections : 4
  IS-IS: Level-2 DR Elections : 4
  IS-IS: Level-1 SPF Calculations : 0
  IS-IS: Level-2 SPF Calculations : 389
  IS-IS: LSP checksum errors received : 0
  IS-IS: LSP authentication failures : 0
Dell#
```

spf-interval

Specify the minimum interval between shortest path first (SPF) calculations.

Syntax

`spf-interval [level-l | level-2]` *`interval seconds`* `[`*`initial_wait_interval seconds`* `[`*`second_wait_interval seconds`*`]]`

To restore default values, use the `no spf-interval [level-l | level-2]` *`interval seconds`* `[`*`initial_wait_interval seconds`* `[`*`second_wait_interval seconds`*`]]` command.

Parameters

level-l	(OPTIONAL) Enter the keyword `level-1` to apply the configuration to Level-1 SPF calculations.

level-2	(OPTIONAL) Enter the keyword `level-2` to apply the configuration to Level-2 SPF calculations.
interval seconds	Enter the maximum number of seconds between SPF calculations. The range is from 0 to 120 seconds. The default is **10 seconds**.
initial_wait_interval seconds	(OPTIONAL) Enter the initial wait time, in seconds, before running the first SPF calculations. The range is from 0 to 120 seconds. The default is **5 seconds**.
second_wait_interval seconds	(OPTIONAL) Enter the wait interval, in seconds, between the first and second SPF calculations. The range is from 0 to 120 seconds. The default is **5 seconds**.

Defaults

Refer to *Parameters*.

Command Modes

- ROUTER ISIS (*for IPv4*)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

This command `spf-interval` in CONFIG-ROUTER-ISIS-AF-IPV6 mode is used for IPv6 Multi-Topology route computation only. If using Single Topology mode, use the `spf-interval` command in CONFIG-ROUTER-ISIS mode for both IPv4 and IPv6 route computations.

SPF throttling slows down the frequency at which route calculations are performed during network instability. Even though throttling route calculations slows down network convergence, not throttling can result in a network not functioning as expected. If network topology is unstable, throttling slows down the scheduling of route calculations until the topology regains its stability.

The first route calculation is controlled by the initial wait interval and the second calculation is controlled by the second wait interval. Each subsequent wait interval is twice as long as the previous one until the wait interval reaches the maximum wait time specified (`interval seconds`). After the network calms down and there are no triggers for two times the maximum interval, fast behavior is restored (the initial wait time).

29

Link Aggregation Control Protocol (LACP)

This chapter contains commands for Dell Networks’s implementation of the link aggregation control protocol (LACP) for creating dynamic link aggregation groups (LAGs) — known as port-channels in the Dell Networking Operating System (OS).

NOTE: For static LAG commands, refer to the Interfaces chapter), based on the standards specified in the IEEE 802.3 Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications.

clear lacp counters

Clear port channel counters.

Syntax

```
clear lacp port-channel-number counters
```

Parameters

port-channel-number	Enter a port-channel number. The range is from 1 to 128.

Defaults

Without a Port Channel specified, the command clears all Port Channel counters.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

show lacp — displays the LACP configuration.

debug lacp

Debug LACP (configuration, events, and so on).

Syntax

```
debug lacp [config | events | pdu [interface [in | out]]]
```

To disable LACP debugging, use the `no [config | events | pdu [interface [in | out]]]` command.

Parameters

config	(OPTIONAL) Enter the keyword `config` to debug the LACP configuration.

events	(OPTIONAL) Enter the keyword `events` to debug the LACP event information.
pdu	(OPTIONAL) Enter the keyword `pdu` to debug the LACP Protocol Data Unit information.
interface in | out	(OPTIONAL) Enter the following keywords and slot/port or number information: • For a Ten-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. Optionally, enter an `in` or `out` parameter: • Receive enter `in` • Transmit enter `out`

Defaults: none

Command Modes:

- EXEC
- EXEC Privilege

Command History:

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

lacp long-timeout

Configure a long timeout period (30 seconds) for an LACP session.

Syntax

```
lacp long-timeout
```

To reset the timeout period to a short timeout (1 second), use the `no lacp long-timeout` command.

Defaults: **1 second**

Command Modes: INTERFACE (conf-if-po-number)

Command History:

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information: This command applies to dynamic port-channel interfaces only. When applied on a static port-channel, this command has no effect.

lacp port-priority

To influence which ports will be put in Standby mode when there is a hardware limitation that prevents all compatible ports from aggregating, configure the port priority.

Syntax

`lacp port-priority` *`priority-value`*

To return to the default setting, use the `no lacp port-priority` *`priority-value`* command.

Parameters

priority-value	Enter the port-priority value. The higher the value number, the lower the priority. The range is from 1 to 65535. The default is **32768**.

Defaults

32768

Command Modes

INTERFACE

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

lacp system-priority

Configure the LACP system priority.

Syntax

`lacp system-priority` *`priority-value`*

Parameters

priority-value	Enter the port-priority value. The higher the value number, the lower the priority. The range is from 1 to 65535. The default is **32768**.

Defaults

32768

Command Modes

INTERFACE

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

port-channel mode

Configure the LACP port channel mode.

Syntax

```
port-channel number mode [active] [passive] [off]
```

Parameters

number	Enter the keywords `number` then a number.
active	Enter the keyword `active` to set the mode to the active state. **NOTE:** LACP modes are defined in *Usage Information*.
passive	Enter the keyword `passive` to set the mode to the passive state. **NOTE:** LACP modes are defined in *Usage Information*.
off	Enter the keyword `off` to set the mode to the off state. **NOTE:** LACP modes are defined in *Usage Information*.

Defaults **off**

Command Modes INTERFACE

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

LACP Modes

Mode	Function
active	An interface is in an active negotiating state in this mode. LACP runs on any link configured in the active state and also automatically initiates negotiation with other ports by initiating LACP packets.
passive	An interface is not in an active negotiating state in this mode. LACP runs on any link configured in the passive state. Ports in a passive state respond to negotiation requests from other ports that are in active states. Ports in a passive state respond to LACP packets
off	An interface cannot be part of a dynamic port channel in off mode. LACP does not run on a port configured in off mode.

port-channel-protocol lacp

Enable LACP on any LAN port.

Syntax

`port-channel-protocol lacp`

To disable LACP on a LAN port, use the `no port-channel-protocol lacp` command.

Command Modes

INTERFACE

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell(conf)#interface TenGigabitethernet 3/15
Dell(conf-if-tengig-3/15)#no shutdown
Dell(conf-if-tengig-3/15)#port-channel-protocol lacp
Dell(conf-if-tengig-3/15-lacp)#port-channel 32 mode active
...
Dell(conf)#interface TenGigabitethernet 3/16
Dell(conf-if-tengig-3/16)#no shutdown
Dell(conf-if-tengig-3/16)#port-channel-protocol lacp
Dell(conf-if-tengig-3/16-lacp)#port-channel 32 mode active
```

show lacp

Display the LACP matrix.

Syntax

`show lacp port-channel-number [sys-id | counters]`

Parameters

port-channel-number	Enter a port-channel number. The range is from 1 to 128.
sys-id	(OPTIONAL) Enter the keywords `sys-id` and the value that identifies a system.
counters	(OPTIONAL) Enter the keyword `counters` to display the LACP counters.

Defaults

Without a Port Channel specified, the command clears all Port Channel counters.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example (Port-Channel-Number)

```
Dell#show lacp 1
Port-channel 1 admin up, oper up, mode lacp
Actor   System ID:Priority 32768, Address 0001.e800.a12b
Partner System ID:Priority 32768, Address 0001.e801.45a5
                  Actor Admin Key 1, Oper Key 1, Partner Oper
Key 1
                  LACP LAG 1 is an aggregatable link

A-Active LACP, B-Passive LACP, C-Short Timeout, D-Long Timeout
E-Aggregatable Link, F-Individual Link, G-IN_SYNC, H-
OUT_OF_SYNC
I-Collection enabled, J-Collection disabled, K-Distribution
enabled L-Distribution disabled,
M-Partner Defaulted, N-Partner Non-defaulted, O-Receiver is in
expired state,
P-Receiver is not in expired state

Port Gi 10/6 is enabled, LACP is enabled and mode is lacp
  Actor   Admin: State ACEHJLMP Key 1    Priority 128
           Oper: State ACEGIKNP Key 1    Priority 128
  Partner Admin: State BDFHJLMP Key 0    Priority 0
           Oper: State BCEGIKNP Key 1    Priority 128
Dell#
```

Example (Sys-id)

```
Dell#show lacp 1 sys-id
Actor    System ID: Priority 32768, Address 0001.e800.a12b
Partner  System ID: Priority 32768, Address 0001.e801.45a5

Dell#
```

Example (Counter)

```
Dell#show lacp 1 counters
----------------------------------------------------
           LACP PDU    Marker PDU   Unknown   Illegal
Port     Xmit Recv   Xmit Recv      Pkts Rx   Pkts Rx
-----------------------------------------------------
Gi 10/6  200  200     0    0         0          0
Dell#
```

Related Commands

clear lacp counters — clears the LACP counters.

show interfaces port-channel — displays information on configured Port Channel groups.

30

Layer 2

This chapter describes commands to configure Layer 2 features.

This chapter contains:

- MAC Addressing Commands

MAC Addressing Commands

The following commands are related to configuring, managing, and viewing MAC addresses.

clear mac-address-table

Clear the MAC address table.

Syntax

```
clear mac-address-table dynamic {address mac-address | all |
interface interface | vlan vlan-id}
```

Parameters

address *mac-address*	Enter the keyword `address` then a MAC address in nn:nn:nn:nn:nn:nn format.
all	Enter the keyword `all` to delete all MAC address entries in the MAC address table.
terface *interface*	Enter the following keywords and slot/port or number information: • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
vlan *vlan-id*	Enter the keyword `vlan` then a VLAN ID number from 1 to 4094.

Command Modes EXEC Privilege

Command History	**Version 8.3.16.1**	Introduced on the MXL 10/40GbE Switch IO Module.

mac-address-table aging-time

Specify an aging time for MAC addresses to remove from the MAC address table.

Syntax `mac-address-table aging-time` *`seconds`*

To delete the configured aging time, use the `no mac-address-table aging-time` *`seconds`* command.

Parameters

seconds	Enter either zero (0) or a number as the number of seconds before MAC addresses are relearned. To disable aging of the MAC address table, enter `0`. The range is from 10 to 1000000. The default is **1800 seconds**.

Defaults **1800 seconds**

Command Modes CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

mac-address-table static

Associate specific MAC or hardware addresses to an interface and virtual local area networks (VLANs).

Syntax `mac-address-table static` *`mac-address`* `output` *`interface`* `vlan` *`vlan-id`*

To remove a MAC address, use the `no mac-address-table static` *`mac-address`* `output` *`interface`* `vlan` *`vlan-id`* command.

Parameters

mac-address	Enter the 48-bit hexadecimal address in nn:nn:nn:nn:nn:nn format.
output *interface*	Enter the keyword `output` then one of the following interfaces for which traffic is forwarded: • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.

	- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
vlan *vlan-id*	Enter the keyword `vlan` then a VLAN ID number from 1 to 4094.

Defaults Not configured.

Command Modes CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

mac-address-table station-move refresh-arp

Ensure that address resolution protocol (ARP) refreshes the egress interface when a station move occurs due to a topology change.

Syntax

```
[no] mac-address-table station-move refresh-arp
```

Defaults none

Command Modes CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information For details about using this command, refer to the “NIC Teaming” section of the Layer 2 chapter in the *Dell Networking OS Configuration Guide*.

mac learning-limit

Limit the maximum number of MAC addresses (static + dynamic) learned on a selected interface.

Syntax

```
mac learning-limit address_limit [dyanmic] [no-station-move|
station-move][sticky]
```

Parameters

address_limit	Enter the maximum number of MAC addresses that can be learned on the interface. The range is from 1 to 1000000.

dynamic	(OPTIONAL) Enter the keyword `dynamic` to allow aging of MACs even though a learning limit is configured.
no-station-move	(OPTIONAL) Enter the keywords `no-station-move` to disallow a station move (associate the learned MAC address with the most recently accessed port) on learned MAC addresses.
station-move	(OPTIONAL) Enter the keywords `station-move` to allow a station move on learned MAC addresses.
sticky	(OPTIONAL) Enter the keyword `sticky` to allow configuring the sticky mac feature along with the learning limit.

Defaults

dynamic

NOTE: "Static" means manually entered addresses, which do not age.

Command Modes

INTERFACE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

This command and its options are supported on physical interfaces, static LAGs, LACP LAGs, and VLANs.

If you do not specify the `vlan` option, the MAC address counters are not VLAN-based. That is, the sum of the addresses learned on all VLANs (not having any learning limit configuration) is counted against the MAC learning limit.

MAC Learning Limit violation logs and actions are not available on a per-VLAN basis.

With the keyword `no-station-move` option, MAC addresses learned through this feature on the selected interface persist on a per-VLAN basis, even if received on another interface. Enabling or disabling this option has no effect on already learned MAC addresses.

After the MAC address learning limit is reached, the MAC addresses do not age out unless you add the `dynamic` option. To clear statistics on MAC address learning, use the `clear counters` command with the learning-limit parameter.

When a channel member is added to a port-channel and there is not enough ACL CAM space, the MAC limit functionality on that port-channel is undefined. When this occurs, un-configure the existing configuration first and then reapply the limit with a lower value.

Related Commands

clear counters — Clear counters used in the `show interface` command.

clear mac-address-table dynamic — clears the MAC address table of all MAC address learned dynamically.

show mac learning-limit — displays MAC learning-limit configuration.

mac learning-limit learn-limit-violation

Configure an action for a MAC address learning-limit violation.

Syntax	`mac learning-limit learn-limit-violation {log | shutdown}` To return to the default, use the `no mac learning-limit learn-limit-violation {log | shutdown}` command.
Parameters	**log** — Enter the keyword `log` to generate a syslog message on a learning-limit violation. **shutdown** — Enter the keyword `shutdown` to shut down the port on a learning-limit violation.
Defaults	none
Command Modes	INTERFACE (conf-if-interface-slot/port)
Command History	**Version 8.3.16.1** — Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	This command is supported on physical interfaces, static LAGs, and LACP LAGs.
Related Commands	show mac learning-limit — displays details of the mac learning-limit.

mac learning-limit station-move-violation

Specify the actions for a station move violation.

Syntax	`mac learning-limit station-move-violation {log | shutdown-both | shutdown-offending | shutdown-original}` To disable a configuration, use the `no mac learning-limit station-move-violation` command, then the configured keyword.
Parameters	**log** — Enter the keyword `log` to generate a syslog message on a station move violation. **shutdown-both** — Enter the keyword `shutdown` to shut down both the original and offending interface and generate a syslog message.

shutdown-offending	Enter the keywords `shutdown-offending` to shut down the offending interface and generate a syslog message.
shutdown-original	Enter the keywords `shutdown-original` to shut down the original interface and generate a syslog message.

Defaults none

Command Modes INTERFACE (conf-if-interface-slot/port)

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information This command is supported on physical interfaces, static LAGs, and LACP LAGs.

Related Commands show mac learning-limit — displays details of the mac learning-limit.

mac learning-limit reset

Reset the MAC address learning-limit error-disabled state.

Syntax `mac learning-limit reset`

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

show cam mac stack-unit

Display the content addressable memory (CAM) size and the portions allocated for MAC addresses and for MAC ACLs.

Syntax

```
show cam mac stack-unit unit_number port-set port-pipe count
[vlan vlan-id] [interface interface]
```

Parameters

stack-unit *unit_number*	(REQUIRED) Enter the keyword `linecard` then a stack member number to select the linecard for which to gather information. The range is 0 to 5.

port-set *port-pipe*	(REQUIRED) Enter the keywords `port-set` then a Port-Pipe number to select the Port-Pipe for which to gather information. The range is 0.
address *mac-addr*	(OPTIONAL) Enter the keyword `address` then a MAC address in the nn:nn:nn:nn:nn:nn format to display information on that MAC address.
dynamic	(OPTIONAL) Enter the keyword `dynamic` to display only those MAC addresses learned dynamically by the switch.
static	(OPTIONAL) Enter the keyword `static` to display only those MAC address specifically configured on the switch.
interface *interface*	(OPTIONAL) Enter the keyword `interface` then the interface type, slot and port information: • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
vlan *vlan-id*	(OPTIONAL) Enter the keyword `vlan` then the VLAN ID to display the MAC address assigned to the VLAN. The range is 1 to 4094.

Command Modes

- EXEC
- EXEC Privilege

Command History		
	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

show mac-address-table

Display the MAC address table.

Syntax

```
show mac-address-table [dynamic | static] [address mac-address
| interface interface | vlan vlan-id] [count [vlan vlan-id]
[interface interface-type [slot [/port]]]]
```

Parameters

dynamic	(OPTIONAL) Enter the keyword `dynamic` to display only those MAC addresses the switch dynamically learns. Optionally, you can also add one of these combinations: `address/`*`mac-address`*, `interface/`*`interface`*, or `vlan` *`vlan-id`*.

static	(OPTIONAL) Enter the keyword `static` to display only those MAC addresses specifically configured on the switch. Optionally, you can also add one of these combinations: `address/`*`mac-address`*, `interface/`*`interface`*, or `vlan` *`vlan-id`*.
address *mac-address*	(OPTIONAL) Enter the keyword `address` then a MAC address in the nn:nn:nn:nn:nn:nn format to display information on that MAC address.
interface *interface*	(OPTIONAL) Enter the keyword `interface` then the interface type, slot and port information: • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
interface *interface-type*	(OPTIONAL) Instead of entering the keyword `interface` then the interface type, slot and port information, as above, you can enter the interface type, then just a slot number.
vlan *vlan-id*	(OPTIONAL) Enter the keyword `vlan` then the VLAN ID to display the MAC address assigned to the VLAN. The range is 1 to 4094.
count	(OPTIONAL) Enter the keyword `count`, then optionally, by an interface or VLAN ID, to display total or interface-specific static addresses, dynamic addresses, and MAC addresses in use.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show mac-address-table` command shown in the following example.

Column Heading	Description
VlanId	Displays the VLAN ID number.
Mac Address	Displays the MAC address in nn:nn:nn:nn:nn:nn format.
Type	Lists whether the MAC address was manually configured (Static), learned dynamically (Dynamic), or associated with a specific port (Sticky).

Column Heading	Description
Interface	Displays the interface type and slot/port information. The following abbreviations describe the interface types: • gi — Gigabit Ethernet then a slot/port. • po — Port Channel then a number. The range is from 1 to 255 for TeraScale. • so —SONET then a slot/port. • te — 10 Gigabit Ethernet then a slot/port.
State	Lists if the MAC address is in use (Active) or not in use (Inactive).

Example

```
Dell#show mac-address-table
VlanId Mac Address       Type     Interface  State
20     00:00:c9:ad:f6:12 Dynamic  Te 0/3     Active
Dell#
```

Usage Information

The following describes the `show mac-address-table` command shown in the following example.

Column Heading	Description
VlanId	Displays the VLAN ID number.
Mac Address	Displays the MAC address in nn:nn:nn:nn:nn:nn format.
Type	Lists whether the MAC address was manually configured (Static), learned (Dynamic), or associated with a specific port (Sticky). An (N) indicates that the specified MAC address has been learnt by a neighbor and is synced to the node.
Interface	Displays the interface type and slot/port information. The following abbreviations describe the interface types: • gi — Gigabit Ethernet then a slot/port • po — Port Channel then a number. The range is from 1 to 255. \ • so — SONET then a slot/port. • te — 10–Gigabit Ethernet then a slot/port.
State	Lists if the MAC address is in use (Active) or not in use (Inactive).

The following describes the `show mac-address-table count` command shown in the following example.

Line Beginning With	Description
MAC Entries...	Displays the number of MAC entries learned per VLAN.

Line Beginning With	Description
Dynamic Address...	Lists the number of dynamically learned MAC addresses.
Static Address...	Lists the number of user-defined MAC addresses.
Total MAC...	Lists the total number of MAC addresses the switch uses.

Example (Count)

```
Dell#show mac-address-table count
MAC Entries for all vlans :
Dynamic Address Count :                  5
Static Address (User-defined) Count :   0
Total MAC Addresses in Use:              5
Dell#
```

Related Commands

show mac-address-table aging-time — displays MAC aging time.

show mac-address-table aging-time

Display the aging times assigned to the MAC addresses on the switch.

Syntax

`show mac-address-table aging-time [vlan vlan-id]`

Parameters

vlan *vlan-id*	(OPTIONAL) Enter the keyword `vlan` then the VLAN ID to display the MAC address assigned to the VLAN. The range is from 1 to 4094.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show mac-address-table aging-time
  Mac-address-table aging time : 1800

Dell#
```

Related Commands

show mac-address-table — displays the current MAC address configuration.

show mac learning-limit

Display MAC address learning limits set for various interfaces.

Syntax

`show mac learning-limit [violate-action] [detail] [interface` *`interface`*`]`

Parameters

violate-action	(OPTIONALY) Enter the keywords `violate-action` to display the MAC learning limit violation status.
detail	(OPTIONAL) Enter the keyword `detail` to display the MAC learning limit in detail.
interface *interface*	(OPTIONAL) Enter the keyword `interface` with the following keywords and slot/port or number information: • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show mac learning-limit
Interface  Learning  Dynamic    Static Unknown   SA
Slot/port  Limit     MAC count  MAC count        Drops
Dell#
```

Virtual LAN (VLAN) Commands

The following commands configure and monitor virtual LANs (VLANs). VLANs are a virtual interface and use many of the same commands as physical interfaces.

You can configure an IP address and Layer 3 protocols on a VLAN called Inter-VLAN routing. FTP, TFTP, ACLs and SNMP are not supported on a VLAN.

Occasionally, while sending broadcast traffic over multiple Layer 3 VLANs, the VRRP state of a VLAN interface may continually switch between Master and Backup.

NOTE: For more information, refer to VLAN Stacking and VLAN-related commands, such as portmode hybrid in the Interfaces chapter.

description

Add a description about the selected VLAN.

Syntax	`description` *`description`*
Parameters	<table><tr><td>**description**</td><td>Enter a text string description to identify the VLAN (80 characters maximum).</td></tr></table>
Defaults	none
Command Modes	INTERFACE VLAN
Command History	<table><tr><td>**Version 8.3.16.1**</td><td>Introduced on the MXL 10/40GbE Switch IO Module.</td></tr></table>
Related Commands	show vlan — displays the VLAN configuration.

default vlan-id

Specify a VLAN as the Default VLAN.

Syntax	`default vlan-id` *`vlan-id`* To remove the default VLAN status from a VLAN and VLAN 1 does not exist, use the `no default vlan-id` *`vlan-id`* syntax.
Parameters	<table><tr><td>***vlan-id***</td><td>Enter the VLAN ID number of the VLAN to become the new Default VLAN. The range is from 1 to 4094. The default is **1**.</td></tr></table>
Defaults	The Default VLAN is VLAN **1**.
Command Modes	CONFIGURATION
Command History	<table><tr><td>**Version 8.3.16.1**</td><td>Introduced on the MXL 10/40GbE Switch IO Module.</td></tr></table>
Usage Information	To return VLAN 1 as the Default VLAN, use the (`default-vlan-id 1`) command. The Default VLAN contains only untagged interfaces.
Related Commands	interface vlan — configures a VLAN.

default-vlan disable

Disable the default VLAN so that all switchports are placed in the Null VLAN until they are explicitly configured as a member of another VLAN.

Defaults	Enabled.
Command Modes	CONFIGURATION
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	The `no default vlan disable` command is not listed in the running-configuration, but when the default VLAN is disabled, `default-vlan disable` is listed in the running-configuration.

name

Assign a name to the VLAN.

Syntax	`name` *`vlan-name`* To remove the name from the VLAN, use the `no name` command.
Parameters	*vlan-name* Enter up to 32 characters as the name of the VLAN.
Defaults	Not configured.
Command Modes	INTERFACE VLAN
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	To display information about a named VLAN, enter the `show vlan` command with the name parameter or the `show interfaces description` command.
Related Commands	description — assigns a descriptive text string to the interface. interface vlan — configures a VLAN. show vlan — displays the current VLAN configurations on the switch.

show config

Display the current configuration of the selected VLAN.

Syntax	`show config`
Command Modes	INTERFACE VLAN
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell(conf-if-vl-100)#show config
!
interface Vlan 1
  description a
  no ip address
  mtu 2500
  shutdown
Dell(conf-if-vl-100)#
```

show vlan

Display the current VLAN configurations on the switch.

Syntax `show vlan [brief | id vlan-id | name vlan-name]`

Parameters

brief	(OPTIONAL) Enter the keyword `brief` to display the following information: • VLAN ID • VLAN name (left blank if none is configured) • Spanning Tree Group ID • MAC address aging time • IP address
id *vlan-id*	(OPTIONAL) Enter the keyword `id` then a number from 1 to 4094. Only information on the VLAN specified is displayed.
name *vlan-name*	(OPTIONAL) Enter the keyword `name` then the name configured for the VLAN. Only information on the VLAN named is displayed.

Command Modes

- EXEC
- EXEC Privilege

Command History	**Version 8.3.16.1**	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show vlan` command shown in the following example.

Column Heading	Description
(Column 1 — no heading)	• asterisk symbol (*) = Default VLAN • G = GVRP VLAN • P = primary VLAN • C = community VLAN • I = isolated VLAN • O = OpenFlow
NUM	Displays existing VLAN IDs.
Status	Displays the word *Inactive* for inactive VLANs and the word *Active* for active VLANs.
Q	• Displays G for GVRP tagged • M for member of a VLAN-Stack VLAN • T for tagged interface • U for untagged interface • x (not capitalized x) for Dot1x untagged • X (capitalized X) for Dot1x tagged • o (not capitalized o) for OpenFlow untagged • O (capitalized O) for OpenFlow tagged • H for VSN tagged • i (not capitalized i) for Internal untagged • I (capitalized I) for Internal tagged • v (not capitalized v) for VLT untagged • V (capitalized V) for VLT tagged
Ports	Displays the type, slot, and port information. • Po = port channel • Gi = gigabit Ethernet • Te = ten-gigabit Ethernet

Example

```
Dell#show vlan

Codes: * - Default VLAN, G - GVRP VLANs, R - Remote Port
Mirroring VLANs, P -
Primary, C - Community, I - Isolated
Q: U - Untagged, T - Tagged
   x - Dot1x untagged, X - Dot1x tagged
   G - GVRP tagged, M - Vlan-stack, H - VSN tagged
   i - Internal untagged, I - Internal tagged, v - VLT
untagged, V - VLT tagged
   NUM  Status    Description Q Ports
   1    Inactive  a
   2    Inactive
```

```
*  20   Active                   U Te 0/3,5,13,53-56
   1002 Active                   T Te 0/3,13,55-56
Dell#
```

Example (VLAN ID)

```
Dell# show vlan id 40

Codes: * - Default VLAN, G - GVRP VLANs, R - Remote Port
Mirroring
VLANs, P - Primary, C - Community, I - Isolated
Q: U - Untagged, T - Tagged
   x - Dot1x untagged, X - Dot1x tagged
   G - GVRP tagged, M - Vlan-stack, H - VSN tagged
   i - Internal untagged, I - Internal tagged, v - VLT
untagged, V
- VLT tagged
   NUM  Status    Description Q Ports
   1    Inactive  a
Dell#
```

Example (Brief)

```
Dell#show vlan brief
VLAN Name STG MAC Aging IP Address
---- ------------------------------
1         0   0         unassigned
2         0   0         unassigned
20        0   0         unassigned
1002      0   0         unassigned
Dell#
```

Example (Name)

```
Dellconf)#interface vlan 222
Dell(conf-if-vl-222)#name test
Dell(conf-if-vl-222)#do show vlan name test

Codes: * - Default VLAN, G - GVRP VLANs
Q: U - Untagged, T - Tagged
   x - Dot1x untagged, X - Dot1x tagged
   G - GVRP tagged, M - Vlan-stack

     NUM  Status Description  Q Ports
     222  Inactive            U Gi 1/22
Dell(conf-if-vl-222)#
```

Related Commands

vlan-stack compatible — enables the Stackable VLAN feature on the selected VLAN.

interface vlan — configures a VLAN.

tagged

Add a Layer 2 interface to a VLAN as a tagged interface.

Syntax

`tagged` *`interface`*

To remove a tagged interface from a VLAN, use the `no tagged` *`interface`* command.

Parameters	*interface*	Enter the following keywords and slot/port or number information: - For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

Defaults All interfaces in Layer 2 mode are untagged.

Command Modes INTERFACE VLAN

Command History	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information When you use the `no tagged` command, the interface is automatically placed in the Default VLAN as an untagged interface unless the interface is a member of another VLAN. If the interface belongs to several VLANs, remove it from all VLANs to change it to an untagged interface.

Tagged interfaces can belong to multiple VLANs, while untagged interfaces can only belong to one VLAN at a time.

In programmable-mux (PMUX) mode of input/output aggregator (IOA), when you use the `no tagged` command on an interface, the VLAN is not removed from the VLAN table, even if there are no active members for the VLAN.

Related Commands interface vlan — configures a VLAN.

untagged — specifies which interfaces in a VLAN are untagged.

track ip

Track the Layer 3 operational state of a Layer 3 VLAN, using a subset of the VLAN member interfaces.

Syntax `track ip` *`interface`*

To remove the tracking feature from the VLAN, use the `no track ip` *`interface`* command.

Parameters	*interface*	Enter the following keywords and slot/port or number information: - For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

Defaults

Not configured.

Command Modes

INTERFACE VLAN

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

When this command is configured, the VLAN is operationally UP if any of the interfaces specified in the `track ip` command are operationally UP, and the VLAN is operationally DOWN if none of the tracking interfaces are operationally UP.

If the `track ip` command is not configured, the VLAN's Layer 3 operational state depends on all the members of the VLAN.

The Layer 2 state of the VLAN, and hence the Layer 2 traffic, is not affected by the `track ip` command configuration.

Related Commands

interface vlan — configures a VLAN.

tagged — specifies which interfaces in a VLAN are tagged.

untagged

Add a Layer 2 interface to a VLAN as an untagged interface.

Syntax

`untagged` *`interface`*

To remove an untagged interface from a VLAN, use the `no untagged` *`interface`* command.

Parameters

interface	Enter the following keywords and slot/port or number information: • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

Defaults

All interfaces in Layer 2 mode are untagged.

Command Modes

INTERFACE VLAN

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Untagged interfaces can only belong to one VLAN.

In the Default VLAN, you cannot use the `no untagged interface` command. To remove an untagged interface from all VLANs, including the Default VLAN, enter INTERFACE mode and use the `no switchport` command.

Related Commands

interface vlan — configures a VLAN.

tagged — specifies which interfaces in a VLAN are tagged.

31

Link Layer Discovery Protocol (LLDP)

Link layer discovery protocol (LLDP) advertises connectivity and management from the local station to the adjacent stations on an IEEE 802 LAN.

LLDP facilitates multi-vendor interoperability by using standard management tools to discover and make available a physical topology for network management. The Dell Networking operating software implementation of LLDP is based on IEEE standard 801.1ab.

The starting point for using LLDP is invoking LLDP with the `protocol lldp` command in either CONFIGURATION or INTERFACE mode.

The information LLDP distributes is stored by its recipients in a standard management information base (MIB). You can access the information by a network management system through a management protocol such as simple network management protocol (SNMP).

For details about implementing LLDP/LLDP-MED, refer to the Link Layer Discovery Protocol chapter of the *Dell Networking OS Configuration Guide*.

advertise dot1-tlv

Advertise dot1 TLVs (Type, Length, Value).

Syntax

`advertise dot1-tlv {port-protocol-vlan-id | port-vlan-id | vlan-name}`

To remove advertised dot1-tlv, use the `no advertise dot1-tlv {port-protocol-vlan-id | port-vlan-id | vlan-name}` command.

Parameters

port-protocol-vlan-id	Enter the keywords `port-protocol-vlan-id` to advertise the port protocol VLAN identification TLV.
port-vlan-id	Enter the keywords `port-vlan-id` to advertise the port VLAN identification TLV.
vlan-name	Enter the keywords `vlan-name` to advertise the vlan-name TLV.

Defaults

Disabled.

Command Modes

CONFIGURATION (conf-lldp) and INTERFACE (conf-if-*interface*-lldp)

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

[protocol lldp (Configuration)]() — enables LLDP globally.

[debug lldp interface]() — debugs LLDP.

[show lldp neighbors]() — displays the LLDP neighbors.

[show running-config lldp]() — displays the LLDP running configuration.

advertise dot3-tlv

Advertise dot3 TLVs (Type, Length, Value).

Syntax

```
advertise dot3-tlv {max-frame-size}
```

To remove advertised dot3-tlv, use the `no advertise dot3-tlv {max-frame-size}` command.

Parameters

max-frame-size	Enter the keywords `max-frame-size` to advertise the dot3 maximum frame size.

Defaults

none

Command Modes

CONFIGURATION (conf-lldp) and INTERFACE (conf-if-*interface*-lldp)

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

advertise management-tlv

Advertise management TLVs (Type, Length, Value).

Syntax

```
advertise management-tlv {system-capabilities | system-
description | system-name}
```

To remove advertised management TLVs, use the `no advertise management-tlv {system-capabilities | system-description | system-name}` command.

Parameters

system-capabilities	Enter the keywords `system-capabilities` to advertise the system capabilities TLVs to the LLDP peer.
system-description	Enter the keywords `system-description` to advertise the system description TLVs to the LLDP peer.
system-name	Enter the keywords `system-name` to advertise the system name TLVs to the LLDP peer.

Defaults none

Command Modes CONFIGURATION (conf-lldp)

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information The command options `system-capabilities`, `system-description`, and `system-name` can be invoked individually or together, in any sequence.

clear lldp counters

Clear LLDP transmitting and receiving counters for all physical interfaces or a specific physical interface.

Syntax `clear lldp counters` *`interface`*

Parameters

interface	Enter the following keywords and slot/port or number information: • For a 10-Gigabit Ethernet interface, enter the keyword `tenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

Defaults none

Command Modes EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

clear lldp neighbors

Clear LLDP neighbor information for all interfaces or a specific interface.

Syntax `clear lldp neighbors {interface}`

Parameters

interface	Enter the following keywords and slot/port or number information: • For a 10-Gigabit Ethernet interface, enter the keyword `tenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

Defaults none

Command Modes EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

debug lldp interface

To display timer events, neighbor additions or deletions, and other information about incoming and outgoing packets, enable LLDP debugging.

Syntax

```
debug lldp interface {interface | all}{events | packet {brief |
detail} {tx | rx | both}}
```

To disable debugging, use the `no debug lldp interface {interface | all}{events} {packet {brief | detail} {tx | rx | both}}` command.

Parameters

interface	Enter the following keywords and slot/port or number information: • For a 10-Gigabit Ethernet interface, enter the keyword `tenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
all	(OPTIONAL) Enter the keyword `all` to display information on all interfaces.
events	(OPTIONAL) Enter the keyword `events` to display major events such as timer events.

packet	(OPTIONAL) Enter the keyword `packet` to display information regarding packets coming in or going out.
brief	(OPTIONAL) Enter the keyword `brief` to display brief packet information.
detail	(OPTIONAL) Enter the keyword `detail` to display detailed packet information.
tx	(OPTIONAL) Enter the keyword `tx` to display transmit-only packet information.
rx	(OPTIONAL) Enter the keyword `rx` to display receive-only packet information.
both	(OPTIONAL) Enter the keyword `both` to display both receive and transmit packet information.

Defaults none

Command Modes EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

disable

Enable or disable LLDP.

Syntax `disable`

To enable LLDP, use the `no disable` command.

Defaults Enabled, that is `no disable`.

Command Modes CONFIGURATION (conf-lldp) and INTERFACE (conf-if-*interface*-lldp)

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

protocol lldp (Configuration) — enables LLDP globally.

debug lldp interface — debugs LLDP.

show lldp neighbors — displays the LLDP neighbors.

hello

Configure the rate at which the LLDP control packets are sent to its peer.

Syntax	`hello seconds` To revert to the default, use the `no hello seconds` command.
Parameters	*seconds* — Enter the rate, in seconds, at which the control packets are sent to its peer. The rate is from 5 to 180 seconds. The default is **30 seconds**.
Defaults	**30 seconds**
Command Modes	CONFIGURATION (conf-lldp) and INTERFACE (conf-if-*interface*-lldp)
Command History	Version 9.2(0.0) — Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only. Version 8.3.16.1 — Introduced on the MXL 10/40GbE Switch IO Module.

mode

To receive or transmit, set LLDP.

Syntax	`mode {tx	rx}` To return to the default, use the `no mode {tx	rx}` command.
Parameters	tx — Enter the keyword `tx` to set the mode to transmit. rx — Enter the keyword `rx` to set the mode to receive.
Defaults	Both **transmit** and **receive**.
Command Modes	CONFIGURATION (conf-lldp) and INTERFACE (conf-if-*interface*-lldp)
Command History	Version 9.2(0.0) — Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

protocol lldp (Configuration) — enables LLDP globally.

show lldp neighbors — displays the LLDP neighbors.

multiplier

Set the number of consecutive misses before LLDP declares the interface dead.

Syntax `multiplier integer`

To return to the default, use the `no multiplier integer` command.

Parameters

integer	Enter the number of consecutive misses before the LLDP declares the interface dead. The range is from 2 to 10.

Defaults **4 x hello**

Command Modes CONFIGURATION (conf-lldp) and INTERFACE (conf-if-*interface*-lldp)

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

protocol lldp (Configuration)

Enable the LLDP globally on the switch.

Syntax `protocol lldp`

To disable LLDP globally on the chassis, use the `no protocol lldp` command.

Defaults Enabled.

Command Modes CONFIGURATION (conf-lldp)

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

protocol lldp (Interface)

Enter the LLDP protocol in INTERFACE mode.

Syntax	`[no] protocol lldp` To return to the global LLDP configuration mode, use the `no protocol lldp` command from Interface mode.
Defaults	LLDP is not enabled on the interface.
Command Modes	INTERFACE (conf-if-*interface*-lldp)
Command History	Version 8.3.16.1
Usage Information	Before LLDP can be configured on an interface, it must be enabled globally from CONFIGURATION mode. This command places you in LLDP mode on the interface; it does not enable the protocol. When you enter the `LLDP` protocol in the Interface context, it overrides global configurations. When you execute the `no protocol lldp` from INTERFACE mode, interfaces begin to inherit the configuration from global LLDP CONFIGURATION mode.

show lldp neighbors

Display LLDP neighbor information for all interfaces or a specified interface.

Syntax	`show lldp neighbors [interface] [detail]`	
Parameters	*interface*	(OPTIONAL) Enter the following keywords and slot/port or number information: • For a 10-Gigabit Ethernet interface, enter the keyword `tenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
	detail	(OPTIONAL) Enter the keyword `detail` to display all the TLV information, remote management IP addresses, timers, and LLDP tx and rx counters.
Defaults	none	
Command Modes	EXEC Privilege	

Command History	**Version 8.3.16.1**	Introduced on MXL 10/40GbE Switch IO Module

Usage Information: Omitting the keyword `detail` displays only the remote chassis ID, Port ID, and Dead Interval.

Example

```
R1(conf-if-gi-1/31)#do show lldp neighbors
Loc PortID Rem  Host Name       Rem     Port Id Rem Chassis Id
--------------------------------------------------------------
Gi 1/21    R2  GigabitEthernet  2/11   00:01:e8:06:95:3e
Gi 1/31    R3  GigabitEthernet  3/11   00:01:e8:09:c2:4a
```

show lldp statistics

Display the LLDP statistical information.

Syntax: `show lldp statistics`

Defaults: none

Command Modes: EXEC Privilege

Command History	**Version 8.3.16.1**	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show lldp statistics
--------- LLDP GLOBAL STATISTICS ON CHASSIS ------------
Total number of neighbors: 2
Last table change time: 1w5d4h, In ticks: 52729764
Total number of Table Inserts: 56
Total number of Table Deletes: 54
Total number of Table Drops: 0
Total number of Table Age Outs: 12
Dell#
```

show running-config lldp

Display the current global LLDP configuration.

Syntax: `show running-config lldp`

Defaults: none

Command Modes: EXEC Privilege

Command History	**Version 8.3.16.1**	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show running-config lldp
!
protocol lldp
  advertise dot1-tlv port-protocol-vlan-id port-vlan-id
  advertise dot3-tlv max-frame-size
  advertise management-tlv system-capabilities system-
description
  hello 15
  multiplier 3
  no disable
Dell#
```

LLDP-MED Commands

The following are the LLDP-MED (Media Endpoint Discovery) commands.

The LLDP-MED commands are an extension of the set of LLDP TLV advertisement commands.

As defined by ANSI/TIA-1057, LLDP-MED provides organizationally specific TLVs (Type Length Value), so that endpoint devices and network connectivity devices can advertise their characteristics and configuration information. The Organizational Unique Identifier (OUI) for the Telecommunications Industry Association (TIA) is 00-12-BB.

- LLDP-MED Endpoint Device — any device that is on an IEEE 802 LAN network edge, can communicate using IP, and uses the LLDP-MED framework.
- LLDP-MED Network Connectivity Device — any device that provides access to an IEEE 802 LAN to an LLDP-MED endpoint device, and supports IEEE 802.1AB (LLDP) and TIA-1057 (LLDP-MED). The Dell Networking system is an LLDP-MED network connectivity device.

Regarding connected endpoint devices, LLDP-MED provides network connectivity devices with the ability to:

- manage inventory
- manage Power over Ethernet (POE)
- identify physical location
- identify network policy

advertise med guest-voice

To advertise a separate limited voice service for a guest user with their own IP telephony handset or other appliances that support interactive voice services, configure the system.

Syntax

`advertise med guest-voice {`*`vlan-id layer2_priority DSCP_value`*`} | {priority-tagged `*`number`*`}`

To return to the default, use the `no advertise med guest-voice {`*`vlan-id layer2_priority DSCP_value`*`} | {priority-tagged `*`number`*`}` command.

Parameters

vlan-id	Enter the VLAN ID. The range is from 1 to 4094.
layer2_priority	Enter the Layer 2 priority. The range is from 0 to 7.
DSCP_value	Enter the DSCP value. The range is from 0 to 63.
priority-tagged *number*	Enter the keywords `priority-tagged` followed the Layer 2 priority. The range is from 0 to 7.

Defaults

Unconfigured.

Command Modes

CONFIGURATION (conf-lldp)

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

protocol lldp (Configuration) — enables LLDP globally.

debug lldp interface — debugs LLDP.

show lldp neighbors — displays the LLDP neighbors.

show running-config lldp — displays the LLDP running configuration.

advertise med guest-voice-signaling

To advertise a separate limited voice service for a guest user when the guest voice control packets use a separate network policy than the voice data, configure the system.

Syntax

```
advertise med guest-voice-signaling {vlan-id layer2_priority
DSCP_value} | {priority-tagged number}
```

To return to the default, use the `no advertise med guest-voice-signaling {vlan-id layer2_priority DSCP_value} | {priority-tagged number}` command.

Parameters

vlan-id	Enter the VLAN ID. The range is from 1 to 4094.
layer2_priority	Enter the Layer 2 priority. The range is from 0 to 7.
DSCP_value	Enter the DSCP value. The range is from 0 to 63.
priority-tagged *number*	Enter the keywords `priority-tagged` then the Layer 2 priority. The range is from 0 to 7.

Defaults

unconfigured.

Command Modes

CONFIGURATION (conf-lldp)

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

debug lldp interface — debugs LLDP.

show lldp neighbors — displays the LLDP neighbors.

show running-config lldp — displays the LLDP running configuration.

advertise med location-identification

To advertise a location identifier, configure the system.

Syntax

```
advertise med location-identification {coordinate-based value |
civic-based value | ecs-elin value}
```

To return to the default, use the `no advertise med location-identification {coordinate-based value | civic-based value | ecs-elin value}` command.

Parameters

coordinate-based *value*	Enter the keywords `coordinate-based` then the coordinated based location in hexadecimal value of 16 bytes.
civic-based *value*	Enter the keywords `civic-based` then the civic based location in hexadecimal format. The range is from 6 to 255 bytes.
ecs-elin *value*	Enter the keywords `ecs-elin` then the Emergency Call Service (ecs) Emergency Location Identification Number (elin) numeric location string. The range is from 10 to 25 characters.

Defaults

unconfigured.

Command Modes

CONFIGURATION (conf-lldp)

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

- ECS — Emergency call service such as defined by TIA or the national emergency numbering association (NENA)
- ELIN — Emergency location identification number, a valid North America Numbering Plan format telephone number supplied for ECS purposes.

Related Commands

debug lldp interface — debugs LLDP.

show lldp neighbors — displays the LLDP neighbors.

show running-config lldp — displays the LLDP running configuration.

advertise med power-via-mdi

To advertise the Extended Power via MDI TLV, configure the system.

Syntax	`advertise med power-via-mdi` To return to the default, use the `no advertise med power-via-mdi` command.
Defaults	unconfigured.
Command Modes	CONFIGURATION (conf-lldp)
Command History	Version 8.3.16.1
Usage Information	Advertise the Extended Power via MDI on all ports that are connected to an 802.3af powered, LLDP-MED endpoint device.
Related Commands	debug lldp interface — debugs LLDP. show lldp neighbors — displays the LLDP neighbors. show running-config lldp — displays the LLDP running configuration.

advertise med softphone-voice

To advertise softphone to enable IP telephony on a computer so that the computer can be used as a phone, configure the system.

Syntax

`advertise med softphone-voice {vlan-id} | {priority-tagged number}`

To return to the default, use the `no advertise med softphone-voice {vlan-id} | {priority-tagged number}` command.

Parameters

vlan-id	Enter the VLAN ID. The range is from 1 to 4094.
priority-tagged *number*	Enter the keywords `priority-tagged` then the Layer 2 priority. The range is from 0 to 7.

Defaults	unconfigured.
Command Modes	CONFIGURATION (conf-lldp)

Command History	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

debug lldp interface — debugs LLDP.

show lldp neighbors — displays the LLDP neighbors.

show running-config lldp — displays the LLDP running configuration.

advertise med streaming-video

To advertise streaming video services for broadcast or multicast-based video, configure the system. This command does not include video applications that rely on TCP buffering.

Syntax

```
advertise med streaming-video {vlan-id} | {priority-tagged
number}
```

To return to the default, use the `no advertise med streaming-video {vlan-id} | {priority-tagged number}` command.

Parameters

vlan-id	Enter the VLAN ID. The range is from 1 to 4094.
priority-tagged *number*	Enter the keywords `priority-tagged` then the Layer 2 priority. The range is from 0 to 7.

Defaults: unconfigured.

Command Modes: CONFIGURATION (conf-lldp)

Command History	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

debug lldp interface — debugs LLDP.

show lldp neighbors — displays the LLDP neighbors.

show running-config lldp — displays the LLDP running configuration.

advertise med video-conferencing

To advertise dedicated video conferencing and other similar appliances that support real-time interactive video, configure the system.

Syntax

```
advertise med video-conferencing {vlan-id} | {priority-tagged
number}
```

To return to the default, use the `no advertise med video-conferencing {vlan-id} | {priority-tagged number}` command.

Parameters

vlan-id	Enter the VLAN ID. The range is from 1 to 4094.
priority-tagged *number*	Enter the keywords `priority-tagged` then the Layer 2 priority. The range is from 0 to 7.

Defaults: unconfigured.

Command Modes: CONFIGURATION (conf-lldp)

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

debug lldp interface — debugs LLDP.

show lldp neighbors — displays the LLDP neighbors.

show running-config lldp — displays the LLDP running configuration.

advertise med voice-signaling

To advertise when voice control packets use a separate network policy than voice data, configure the system.

Syntax

`advertise med voice-signaling {vlan-id} | {priority-tagged number}`

To return to the default, use the `no advertise med voice-signaling {vlan-id} | {priority-tagged number}` command.

Parameters

vlan-id	Enter the VLAN ID. The range is from 1 to 4094.
priority-tagged *number*	Enter the keywords `priority-tagged` then the Layer 2 priority. The range is from 0 to 7.

Defaults: unconfigured.

Command Modes: CONFIGURATION (conf-lldp)

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

debug lldp interface — debugs LLDP.

show lldp neighbors — displays the LLDP neighbors.

show running-config lldp — displays the LLDP running configuration.

advertise med voice

To advertise a dedicated IP telephony handset or other appliances supporting interactive voice services, configure the system.

Syntax

`advertise med voice {vlan-id} | {priority-tagged number}`

To return to the default, use the `no advertise med voice {vlan-id} | {priority-tagged number}` command.

Parameters

vlan-id	Enter the VLAN ID. The range is from 1 to 4094.
priority-tagged *number*	Enter the keywords `priority-tagged` then the Layer 2 priority. The range is from 0 to 7.

Defaults

unconfigured.

Command Modes

CONFIGURATION (conf-lldp)

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

debug lldp interface — debugs LLDP.

show lldp neighbors — displays the LLDP neighbors.

show running-config lldp — displays the LLDP running configuration.

advertise med voice-signaling

To advertise when voice control packets use a separate network policy than voice data, configure the system.

Syntax

`advertise med voice-signaling {vlan-id} | {priority-tagged number}`

To return to the default, use the `no advertise med voice-signaling {vlan-id} | {priority-tagged number}` command.

Parameters

vlan-id	Enter the VLAN ID. The range is from 1 to 4094.
priority-tagged *number*	Enter the keywords `priority-tagged` then the Layer 2 priority. The range is from 0 to 7.

Defaults	unconfigured.
Command Modes	CONFIGURATION (conf-lldp)
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	debug lldp interface — debugs LLDP. show lldp neighbors — displays the LLDP neighbors. show running-config lldp — displays the LLDP running configuration.

32

Microsoft Network Load Balancing

This functionality is supported on the MXL platforms.

Network Load Balancing (NLB) is a clustering functionality that is implemented by Microsoft on Windows 2000 Server and Windows Server 2003 operating systems. NLB uses a distributed methodology or pattern to equally split and balance the network traffic load across a set of servers that are part of the cluster or group. NLB combines the servers into a single multicast group and attempts to use the standard multicast IP or unicast IP addresses, and MAC addresses for the transmission of network traffic. At the same time, it also uses a single virtual IP address for all clients as the destination IP address, which enables servers to join the same multicast group in a way that is transparent to the clients (the clients do not notice the addition of new servers to the group). The clients use a cluster IP address to connect to the server. The NLB functionality enables flooding of traffic over the VLAN ports (for unicast mode) or a subset of ports in a VLAN (for multicast mode) to avoid overloading and effective performance of the servers for optimal processing of data packets.

NLB functions in two modes, namely unicast mode and multicast mode. The cluster IP address and the associated cluster MAC address are configured in the NLB application running on the Windows Server. In the unicast mode, when the server IP address is attempted to be resolved to the MAC address using the ARP application, the switch determines whether the ARP reply, obtained from the server, is of an NLB type. The switch then maps the IP address (cluster IP) with the MAC address (cluster MAC address). In multicast mode, the cluster IP address is mapped to a cluster multicast MAC address that is configured using a static ARP CLI configuration command. After the NLB entry is learned, the traffic is forwarded to all the servers in the VLAN corresponding to the cluster virtual IP address.

NLB Unicast Mode Scenario

Consider a sample topology in which four servers, namely S1 through S4, are configured as a cluster or a farm. This set of servers is connected to a Layer 3 switch, which in turn is connected to the end-clients. The servers contain a single IP address (IP-cluster address of 172.16.2.20) and a single unicast MAC address (MAC-Cluster address of 00-bf-ac-10-00-01) for load-balancing. Because multiple ports of a switch cannot learn a single MAC address, the servers are assigned with MAC addresseses of MAC-s1 to MAC-s4) respectively on S1 through S4 in addition to the MAC cluster address. All the servers of the cluster belong to the VLAN named VLAN1.

In unicast NLB mode, the following sequence of events occurs:

- The switch sends an ARP request to resolve the IP address to the cluster MAC address.
- The ARP servers send an ARP response with the MAC cluster address in the ARP header and a MAC address of MAC-s1/s2/s3/s4 (for servers S1 through S4) in the Ethernet header.
- The switch associates the IP address with the MAC cluster address with the last ARP response it obtains. Assume that in this case, the last ARP reply is obtained from MAC-s4.(assuming that the ARP

response with MAC-s4 is received as the last one). The interface associated with server, S4, is added to the ARP table.

- With NLB feature enabled, after learning the NLB ARP entry, all the subsequent traffic is flooded on all ports in VLAN1.

With NLB, the data frame is forwarded to all the servers for them to perform load-balancing.

NLB Multicast Mode Scenario

Consider a sample topology in which four servers, namely S1 through S4, are configured as a cluster or a farm. This set of servers is connected to a Layer 3 switch, which in turn is connected to the end-clients. They contain a single multicast MAC address (MAC-Cluster: 03-00-5E-11-11-11).

In the multicast NLB mode, a static ARP configuration command is configured to associate the cluster IP address with a multicast cluster MAC address.

With multicast NLB mode, the data is forwarded to all the servers based on the port specified using the Layer 2 multicast command, which is the `mac-address-table static <multicast_mac> multicast vlan <vlan_id> output-range <port1>, <port2>` command in CONFIGURATION mode.

Limitations With Enabling NLB on Switches

The following limitations apply to switches on which you configure NLB:

- The NLB unicast mode uses switch flooding to transmit all packets to all the servers that are part of the VLAN. When a large volume of traffic is processed, the clustering performance might be impacted in a small way. This limitation is applicable to switches that perform unicast flooding in the software.
- The `ip vlan-flooding` command applies globally across the system and for all VLANs. In cases where the NLB is applicable and the ARP replies contain a discrepancy in the Ethernet SHA and ARP header SHA frames, a flooding of packets over the relevant VLAN occurs.
- The maximum number of concurrent clusters that is supported is eight.

Benefits and Working of Microsoft Clustering

Microsoft clustering allows multiple servers using Microsoft Windows to be represented by one MAC address and IP address in order to provide transparent failover or balancing. Dell Networking OS does not recognize server clusters by default; it must be configured to do so. When an ARP request is sent to a server cluster, either the active server or all the servers send a reply, depending on the cluster configuration. If the active server sends a reply, the Dell switch learns the active server's MAC address. If all servers reply, the switch registers only the last received ARP reply, and the switch learns one server's actual MAC address; the virtual MAC address is never learned. Because the virtual MAC address is never learned, traffic is forwarded to only one server rather than the entire cluster, and failover and balancing are not preserved.

To preserve failover and balancing, the switch forwards the traffic destined for the server cluster to all member ports in the VLAN connected to the cluster. To ensure that this happens, you must configure the `ip vlan-flooding` command on the Dell switch at the time that the Microsoft cluster is configured. The server MAC address is given in the Ethernet frame header of the ARP reply, while the virtual MAC address representing the cluster is given in the payload. Then, all the traffic destined for the cluster is flooded out of all member ports. Since all the servers in the cluster receive traffic, failover and balancing are preserved.

Enable and Disable VLAN Flooding

- The older ARP entries are overwritten whenever newer NLB entries are learned.
- All ARP entries, learned after the feature is enabled, are deleted when the feature is disabled, and RP2 triggers an ARP resolution. The feature is disabled with the `no ip vlan-flooding` command.
- When a port is added to the VLAN, the port automatically receives traffic if the feature is enabled. Old ARP entries are not deleted or updated.
- When a member port is deleted, its ARP entries are also deleted from the CAM.
- Port channels in the VLAN also receive traffic.
- There is no impact on the configuration from saving the configuration.
- The feature, if enabled, is displayed in the `show running-config` command output that displays the `ip vlan-flooding` CLI configuration. Apart from it, there is no indication of the enabling of this capability.

mac-address-table static (for Multicast MAC Address)

For multicast mode of network load balancing (NLB), configure a static multicast MAC address, associate the multicast MAC address with the VLAN used to switch Layer 2 multicast traffic, and add output ports that will receive multicast streams on the VLAN. To delete a configured static multicast MAC address from the MAC address table on the router, enter the `no mac-address-table static` *`multicast-mac-address`* command.

Syntax

```
mac-address-table static multicast-mac-address multicast vlan
vlan-id range-output {single-interface | interface-list |
interface-range}
```

To remove a MAC address, use the `no mac-address-table static` *`multicast-mac-address`* `output` *`interface`* `vlan` *`vlan-id`* command.

Parameters

multicast-mac-address	Enter the 48-bit hexadecimal address in nn:nn:nn:nn:nn:nn format.
multicast	Enter a vlan port to where L2 multicast MAC traffic is forwarded.

> **NOTE:** Use this option if you want multicast functionality in an L2 VLAN without IGMP protocols.

`output` *interface*	For a multicast MAC address, enter the keyword `output` then one of the following interfaces for which traffic is forwarded: • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
`output-range` *interface*	For a multicast MAC address, enter the keyword `output-range` then one of the following interfaces to indicate a range of ports for which traffic is forwarded: • For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the slot/port information. • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
vlan *vlan-id*	Enter the keyword `vlan` then a VLAN ID number from 1 to 4094.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

Version 9.3(0.0)	Added support for multicast MAC address on the MXL platform.

Usage Information

When a multicast source and multicast receivers are in the same VLAN, you can configure a router so that multicast traffic is switched only to the ports assigned to a VLAN that is associated with a static multicast MAC address. However, before you can configure a static MAC address and associate it with a VLAN used to switch Layer 2 multicast traffic, you must first enable the router for Layer 2 multicast switching with the `ip multicast-mode l2` command.

Example (Multicast)

```
mac-address-table static 01:00:5E:01:00:01 {multicast vlan
2 output—range Te 0/2,Te 0/3}
```

ip vlan-flooding

Enable unicast data traffic flooding on VLAN member ports.

Syntax	`ip vlan-flooding` To disable, use the `no ip vlan-flooding` command.
Command Modes	CONFIGURATION
Command History	**Version 9.3(0.0)** Introduced on the MXL 10/40GbE Switch IO Module platform.
Default	Disabled
Usage Information	By default this command is disabled. There might be some ARP table entries which are resolved through ARP packets which had Ethernet MAC SA different from MAC information inside the ARP packet. This unicast data traffic flooding occurs only for those packets which use these ARP entries.

33

Multicast Source Discovery Protocol (MSDP)

Multicast source discovery protocol (MSDP) connects multiple PIM Sparse-Mode (PIM-SM) domains together.

MSDP peers connect using TCP port 639. Peers send keepalives every 60 seconds. A peer connection is reset after 75 seconds if no MSDP packets are received. MSDP connections are parallel with MBGP connections.

clear ip msdp peer

Reset the TCP connection to the peer and clear all the peer statistics.

Syntax `clear ip msdp peer {peer address}`

Parameters

peer address	Enter the peer address in a dotted decimal format (A.B.C.D.)

Defaults Not configured.

Command Modes EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

clear ip msdp sa-cache

Clears the entire source-active cache, the source-active entries of a particular multicast group, rejected, or local source-active entries.

Syntax `clear ip msdp sa-cache [group-address | rejected-sa | local]`

Parameters

group-address	Enter the group IP address in dotted decimal format (A.B.C.D.).
rejected-sa	Enter the keywords `rejected-sa` to clear the cache source-active entries that are rejected because the RPF check failed, an SA filter or limit is configured, the RP or MSDP peer is unreachable, or because of a format error.

	local	Enter the keyword `local` to clear out local PIM advertised entries. It applies the redistribute filter (if present) while adding the local PIM SA entries to the SA cache.

Defaults	Without any options, this command clears the entire source-active cache.
Command Modes	EXEC Privilege
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.

clear ip msdp statistic

Clears the entire source-active cache, the source-active entries of a particular multicast group, rejected, or local source-active entries.

Syntax

```
clear ip msdp sa-cache [group-address | rejected-sa | local]
```

Parameters

group-address	Enter the group IP address in dotted decimal format (A.B.C.D.).
rejected-sa	Enter the keyword `rejected-sa` to clear the cache source-active entries that are rejected because the RPF check failed, an SA filter or limit is configured, the RP or MSDP peer is unreachable, or because of a format error.
local	Enter the keyword `local` to clear out local PIM advertised entries. It applies the redistribute filter (if present) while adding the local PIM SA entries to the SA cache.

Defaults	Without any options, this command clears the entire source-active cache.
Command Modes	EXEC Privilege
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.

debug ip msdp

Turn on MSDP debugging.

Syntax

```
debug ip msdp {event peer address | packet peer address | pim}
```

To turn debugging off, use the `no debug ip msdp {event peer address | packet peer address | pim}` command.

Parameters

event *peer address*	Enter the keyword `event` then the peer address in a dotted decimal format (A.B.C.D.).
packet *peer address*	Enter the keyword `packet` then the peer address in a dotted decimal format (A.B.C.D.).
pim	Enter the keyword `pim` to debug advertisement from PIM.

Defaults — Not configured.

Command Modes — EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

ip msdp cache-rejected-sa

Enable an MSDP cache for the rejected source-active entries.

Syntax — `ip msdp cache-rejected-sa {number}`

To clear the MSDP rejected source-active entries, use the `no ip msdp cache-rejected-sa {number}` command then the `ip msdp cache-rejected-sa {number}` command.

Parameters

number	Enter the number of rejected SA entries to cache. The range is from 0 to 32766.

Defaults — none

Command Modes — CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands — show ip msdp sa-cache rejected-sa — Displays the rejected SAs in the SA cache.

ip msdp default-peer

Define a default peer from which to accept all source-active (SA) messages.

Syntax — `ip msdp default-peer peer address [list name]`

To remove the default peer, use the `no ip msdp default-peer {peer address} list name` command.

Parameters

peer address	Enter the peer address in a dotted decimal format (A.B.C.D.)
list *name*	Enter the keywords `list name` and specify a standard access list that contains the RP address that should be treated as the default peer. If no access list is specified, then all SAs from the peer are accepted.

Defaults: Not configured.

Command Modes: CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information: If a list is not specified, all SA messages received from the default peer are accepted. You can enter multiple `default peer` commands.

ip msdp log-adjacency-changes

Enable logging of MSDP adjacency changes.

Syntax: `ip msdp log-adjacency-changes`

To disable logging, use the `no ip msdp log-adjacency-changes` command.

Defaults: Not configured.

Command Modes: CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

ip msdp mesh-group

To be a member of a mesh group, configure a peer.

Syntax: `ip msdp mesh-group {name} {peer address}`

To remove the peer from a mesh group, use the `no ip msdp mesh-group {name} {peer address}` command.

Parameters

name	Enter a string of up to 16 characters long for as the mesh group name.
peer address	Enter the peer address in a dotted decimal format (A.B.C.D.).

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

An MSDP mesh group is a mechanism for reducing SA flooding, typically in an intra-domain setting. When some subset of a domain's MSDP speakers are fully meshed, they can be configured into a mesh-group. If member X of a mesh-group receives a SA message from an MSDP peer that is also a member of the mesh-group, member X accepts the SA message and forwards it to all of its peers that are not part of the mesh-group. However, member X cannot forward the SA message to other members of the mesh-group.

ip msdp originator-id

Configure the MSDP Originator ID.

Syntax

`ip msdp originator-id {`*`interface`*`}`

To remove the originator-id, use the `no ip msdp originator-id {`*`interface`*`}` command.

Parameters

interface	Enter the following keywords and slot/port or number information: • For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383. • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a SONET interface, enter the keywords `sonet` then the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

ip msdp peer

Configure an MSDP peer.

Syntax

`ip msdp peer` *`peer address`* `[connect-source] [description] [sa-limit` *`number`*`]`

To remove the MSDP peer, use the `no ip msdp peer` *`peer address`* `[connect-source` *`interface`*`] [description` *`name`*`] [sa-limit` *`number`*`]` command.

Parameters

peer address	Enter the peer address in a dotted decimal format (A.B.C.D.).
connect-source *interface*	Enter the keywords `connect-source` then one of the interfaces and slot/port or number information: • For a Fast Ethernet interface, enter the keyword `FastEthernet` then the slot/ port information. • For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383. • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.
description name	(OPTIONAL) Enter the keyword *description* then a description name (maximum 80 characters) to designate a description for the MSDP peer.
sa-limit *number*	(OPTIONAL) Enter the maximum number of SA entries in SA-cache. The range is from 1 to 500000. The default it **500000**.

Defaults

As described in the *Parameters* section.

Command Modes

CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The `connect-source` option is used to supply a source IP address for the TCP connection. When an interface is specified using the `connect-source` option, the primary configured address on the interface is used.

If the total number of SA messages received from the peer is already larger than the limit when this command is applied, those SA messages continue to be accepted. To enforce the limit in such situation, use the `clear ip msdp peer` command to reset the peer.

Related Commands	ip msdp sa-limit — configures the MSDP SA Limit. clear ip msdp peer — clears the MSDP peer. show ip msdp — displays the MSDP information.

ip msdp redistribute

Filter local PIM SA entries in the SA cache. SAs which the ACL denies time out and are not refreshed. Until they time out, they continue to reside in the MSDP SA cache.

Syntax

`ip msdp redistribute [list acl-name]`

Parameters

list *acl-name*	lEnter the name of an extended ACL that contains permitted SAs. If you do not use this option, all local entries are blocked.

Defaults	Not configured.
Command Modes	CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Modifications to the ACL do not have an immediate effect on the sa-cache.

To apply the redistribute filter to entries already present in the SA cache, use the `clear ip msdp sa-cache local` command.

ip msdp sa-filter

Permit or deny MSDP source active (SA) messages based on multicast source and/or group from the specified peer.

Syntax

`ip msdp sa-filter {in | out} peer-address list [access-list name]`

Remove this configuration using the `no ip msdp sa-filter {in | out} peer address list [access-list name]` command.

Parameters

in	Enter the keyword `in` to enable incoming SA filtering.
out	Enter the keyword `out` to enable outgoing SA filtering.

peer-address	Enter the peer address of the MSDP peer in a dotted decimal format (A.B.C.D.).
access-list name	Enter the name of an extended ACL that contains permitted SAs. If you do not use this option, all local entries are blocked.

Defaults: Not configured.

Command Modes: CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

ip msdp sa-limit

Configure the upper limit of source-active (SA) entries in SA-cache.

Syntax

```
ip msdp sa-limit number
```

To return to the default, use the `no ip msdp sa-limit number` command.

Parameters

number	Enter the maximum number of SA entries in SA-cache. The range is from 0 to 40000.

Defaults: **50000**

Command Modes: CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The system counts the SA messages originated by itself and those messages received from the MSDP peers. When the total SA messages reach this limit, the subsequent SA messages are dropped (even if they pass RPF checking and policy checking).

If the total number of SA messages is already larger than the limit when this command is applied, those SA messages that are already in the software continue to be accepted. To enforce the limit in such situation, use the `clear ip msdp sa-cache` command.

Related Commands

ip msdp peer — configures the MSDP peer.

clear ip msdp peer — clears the MSDP peer.

show ip msdp — displays the MSDP information

ip msdp shutdown

Administratively shut down a configured MSDP peer.

Syntax	`ip msdp shutdown {`*`peer address`*`}`
Parameters	
	peer address — Enter the peer address in a dotted decimal format (A.B.C.D.).
Defaults	Not configured.
Command Modes	CONFIGURATION
Command History	Version 9.2(0.0) — Introduced on the MXL 10/40GbE Switch IO Module.

ip multicast-msdp

Enable MSDP.

Syntax	`ip multicast-msdp` To exit MSDP, use the `no ip multicast-msdp` command.
Defaults	Not configured.
Command Modes	CONFIGURATION
Command History	Version 9.2(0.0) — Introduced on the MXL 10/40GbE Switch IO Module.

show ip msdp

Display the MSDP peer status, SA cache, or peer summary.

Syntax	`show ip msdp {peer `*`peer address`*`	sa-cache	summary}`	
Parameters	peer *peer address*	Enter the keyword `peer` then the peer address in a dotted decimal format (A.B.C.D.).
	sa-cache	Enter the keywords `sa-cache` to display the Source-Active cache.
	summary	Enter the keyword `summary` to display an MSDP peer summary.
Defaults	Not configured.	

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show ip msdp peer 100.1.1.1

Peer Addr: 100.1.1.1
  Local Addr: 100.1.1.2(639) Connect Source: none
  State: Established Up/Down Time: 00:00:08
  Timers: KeepAlive 60 sec, Hold time 75 sec
  SourceActive packet count (in/out): 0/0
  SAs learned from this peer: 0
  SA Filtering:
  Input (S,G) filter: none
  Output (S,G) filter: none
Dell#
```

Example (Sa-cache)

```
Dell#show ip msdp sa-cache
MSDP Source-Active Cache - 1 entries
GroupAddr  SourceAddr     RPAddr        LearnedFrom Expire
UpTime
224.1.1.1  172.21.220.10  172.21.3.254  172.21.3.254 102
00:02:52
Dell#
```

Example (Summary)

```
Dell#show ip msdp summary
Peer Addr  Local Addr State      Source SA  Up/Down Description
72.30.1.2  72.30.1.1  Established  none 0  00:00:03 peer1
72.30.2.2  72.30.2.1  Established  none 0  00:00:03 peer2
72.30.3.2  72.30.3.1  Established  none 0  00:00:02 test-peer-3
Dell#
```

show ip msdp sa-cache rejected-sa

Display the rejected SAs in the SA cache.

Syntax

```
show ip msdp sa-cache rejected-sa
```

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#sh ip msdp sa-cache rejected-sa
MSDP Rejected SA Cache 200 rejected SAs received, cache-size
1000
UpTime   GroupAddr SourceAddr RPAddr    LearnedFrom Reason
```

```
00:00:13 225.1.2.1 10.1.1.3   110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.2 10.1.1.4   110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.3 10.1.1.3   110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.4 10.1.1.4   110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.5 10.1.1.3   110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.6 10.1.1.4   110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.7 10.1.1.3   110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.8 10.1.1.4   110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.9 10.1.1.3   110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.10 10.1.1.4  110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.11 10.1.1.3  110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.11 10.1.1.3  110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.12 10.1.1.4  110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.13 10.1.1.3  110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.14 10.1.1.4  110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.15 10.1.1.3  110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.16 10.1.1.4  110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.17 10.1.1.3  110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.18 10.1.1.4  110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.19 10.1.1.3  110.1.1.1 13.1.1.2 Rpf-Fail
Dell#
```

34

Multiple Spanning Tree Protocol (MSTP)

Multiple spanning tree protocol (MSTP), as implemented by the Dell Networking Operating System (OS), conforms to IEEE 802.1s.

debug spanning-tree mstp

Enable debugging of the multiple spanning tree protocol and view information on the protocol.

Syntax

```
debug spanning-tree mstp [all | bpdu interface {in | out} |
events]
```

Parameters

all	(OPTIONAL) Enter the keyword all to debug `all` spanning tree operations.
bpdu *interface* {in | out}	(OPTIONAL) Enter the keyword `bpdu` to debug bridge protocol data units (BPDU). (OPTIONAL) Enter the interface keyword along with the type slot/port of the interface you want displayed. Type slot/port options are the following: • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. Optionally, enter an `in` or `out` parameter with the optional interface: • For Receive, enter the keyword `in`. • For Transmit, enter the keyword `out`.
events	(OPTIONAL) Enter the keyword `events` to debug MSTP events.

Command Modes

EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#debug spanning-tree mstp bpdu tengigabitethernet 0/16 ?
in Receive (in)
out Transmit (out)
Dell#
```

description

Enter a description of the multiple spanning tree.

Syntax

`description {description}`

To remove the description, use the `no description {description}` command.

Parameters

description	Enter a description to identify the multiple spanning tree (maximum 80 characters).

Defaults

none

Command Modes

SPANNING TREE (The prompt is “config-mstp”.)

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

protocol spanning-tree mstp — enters MULTIPLE SPANNING TREE mode on the switch.

disable

Globally disable the multiple spanning tree protocol on the switch.

Syntax

`disable`

To enable MSTP, enter the `no disable` command.

Defaults

disabled.

Command Modes

MULTIPLE SPANNING TREE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

protocol spanning-tree mstp — enters MULTIPLE SPANNING TREE mode.

disable

Enable bridge protocol data units (BPDU) filter globally to filter transmission of BPDU on port-fast enabled interfaces.

Syntax

`edge-port bpdufilter default`

To disable global bpdu filter default, use the `no edge-port bpdufilter default` command.

Defaults

disabled.

Command Modes

MULTIPLE SPANNING TREE

Command History

Version 8.3.16.1	Introduced on MXL 10/40GbE Switch IO Module

forward-delay

The amount of time the interface waits in the Blocking State and the Learning State before transitioning to the Forwarding State.

Syntax

`forward-delay` *`seconds`*

To return to the default setting, use the `no forward-delay` command.

Parameters

seconds	Enter the number of seconds the interface waits in the Blocking State and the Learning State before transiting to the Forwarding State. The range is from 4 to 30. The default is **15 seconds**.

Defaults

15 seconds

Command Modes

MULTIPLE SPANNING TREE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

max-age — changes the wait time before MSTP refreshes protocol configuration information.

hello-time — changes the time interval between bridge protocol data units (BPDUs).

hello-time

Set the time interval between generation of MSTB bridge protocol data units (BPDUs).

Syntax	`hello-time seconds` To return to the default value, use the `no hello-time` command.
Parameters	*seconds* — Enter a number as the time interval between transmission of BPDUs. The range is from 1 to 10. The default is **2 seconds**.
Defaults	**2 seconds**
Command Modes	MULTIPLE SPANNING TREE
Command History	Version 8.3.16.1 — Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	edge-port bpdufilter default — the amount of time the interface waits in the Blocking State and the Learning State before transitioning to the Forwarding State. max-age — changes the wait time before MSTP refreshes protocol configuration information.

max-age

To maintain configuration information before refreshing that information, set the time interval for the MSTB.

Syntax	`max-age seconds` To return to the default values, use the `no max-age` command.
Parameters	*max-age* — Enter a number of seconds the system waits before refreshing configuration information. The range is from 6 to 40. The default is **20 seconds**.
Defaults	**20 seconds**
Command Modes	MULTIPLE SPANNING TREE
Command History	Version 8.3.16.1 — Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	edge-port bpdufilter default — the amount of time the interface waits in the Blocking State and the Learning State before transitioning to the Forwarding State.

hello-time — changes the time interval between BPDUs.

max-hops

Configure the maximum hop count.

Syntax	`max-hops number` To return to the default values, use the `no max-hops` command.
Parameters	range: Enter a number for the maximum hop count. The range is from 1 to 40. The default is **20**.
Defaults	**20 hops**
Command Modes	MULTIPLE SPANNING TREE
Command History	Version 8.3.16.1: Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	The `max-hops` command is a configuration command that applies to both the IST and all MST instances in the MSTP region. The BPDUs sent out by the root switch set the remaining-hops parameter to the configured value of max-hops. When a switch receives the BPDU, it decrements the received value of the remaining hops and uses the resulting value as remaining-hops in the BPDUs. If the remaining-hops reach zero, the switch discards the BPDU and ages out any information that it holds for the port.

msti

Configure multiple spanning tree instance, bridge priority, and one or multiple VLANs mapped to the MST instance.

Syntax

`msti instance {vlan range | bridge-priority priority}`

To disable mapping or bridge priority, use the `no msti instance {vlan range | bridge-priority priority}` command.

Parameters

msti *instance*	Enter the MSTP iInstance. The range is from zero (0) to 63.
vlan *range*	Enter the keyword `vlan` then the identifier range value. The range is from 1 to 4094.
bridge-priority *priority*	Enter the keywords `bridge-priority` then a value in increments of 4096 as the bridge priority. The range is from zero (0) to 61440.

Valid priority values are: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected.

Defaults	default bridge-priority is **32768**.
Command Modes	INTERFACE
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	By default, all VLANs are mapped to MST instance zero (0) unless you use the `vlan` *`range`* command to map it to a non-zero instance. Although MSTP instance IDs range from 0 to 4094, only 64 active instances are supported on the switch.

name

The name you assign to the multiple spanning tree region.

Syntax	`name` *`region-name`* To remove the region name, use the `no name` command.
Parameters	***region-name*** Enter the MST region name. The range is 32 character limit.
Defaults	no default name.
Command Modes	MULTIPLE SPANNING TREE
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	For two MSTP switches to be within the same MSTP region, the switches must share the same region name (including matching case).
Related Commands	msti — maps the VLAN(s) to an MST instance. revision — assigns the revision number to the MST configuration.

protocol spanning-tree mstp

To enable and configure the multiple spanning tree group, enter MULTIPLE SPANNING TREE mode.

Syntax	`protocol spanning-tree mstp` To disable the multiple spanning tree group, use the `no protocol spanning-tree mstp` command.
Defaults	Not configured.
Command Modes	CONFIGURATION
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	MSTP is not enabled when you enter MULTIPLE SPANNING TREE mode. To enable MSTP globally on the switch, enter the `no disable` command while in MULTIPLE SPANNING TREE mode. For more information about the multiple spanning tree protocol, refer to the *Dell Networking OS Configuration Guide*.

Example

```
Dell(conf)#protocol spanning-tree mstp
Dell(config-mstp)#no disable
```

Related Commands	disable — disables multiple spanning tree.

revision

The revision number for the multiple spanning tree configuration.

Syntax	`revision` *`range`* To return to the default values, use the `no revision` command.
Parameters	*range* — Enter the revision number for the MST configuration. The range is from 0 to 65535. The default is **0**.
Defaults	**0**
Command Modes	MULTIPLE SPANNING TREE
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information	For two MSTP switches to be within the same MST region, the switches must share the same revision number.
Related Commands	msti — maps the VLAN(s) to an MST instance. name — assigns the region name to the MST region.

show config

View the current configuration for the mode. Only non-default values are shown.

Syntax	`show config`
Command Modes	MULTIPLE SPANNING TREE
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell(conf-mstp)#show config
!
protocol spanning-tree mstp
  no disable
  name CustomerSvc
  revision 2
  MSTI 10 VLAN 101-105
  max-hops 5
Dell(conf-mstp)#
```

show spanning-tree mst configuration

View the multiple spanning tree configuration.

Syntax	`show spanning-tree mst configuration`
Command Modes	- EXEC - EXEC Privilege
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	Enable the multiple spanning tree protocol prior to using this command.

Example

```
Dell#show spanning-tree mst configuration
MST region name: CustomerSvc
Revision: 2
MSTI VID
```

```
  10 101-105
Dell#
```

show spanning-tree msti

View the multiple spanning tree instance.

Syntax `show spanning-tree msti [instance-number [brief]] [guard]`

Parameters

instance-number	(Optional) Enter the multiple spanning tree instance number. The range is from 0 to 63.
brief	(Optional) Enter the keyword `brief` to view a synopsis of the MST instance.
guard	(Optional) Enter the keyword `guard` to display the type of guard enabled on an MSTP interface and the current port state.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information Enable the multiple spanning tree protocol prior to using this command.

Example

```
Dell#show spanning-tree msti 0 brief
MSTI 0 VLANs mapped 1-4094
Executing IEEE compatible Spanning Tree Protocol
Root ID Priority 32768, Address 0001.e800.0204
Root Bridge hello time 2, max age 20, forward delay 15, max
hops 20
Bridge ID Priority 32768, Address 0001.e800.0204
We are the root of MSTI 0 (CIST)
Configured hello time 2, max age 20, forward delay 15, max
hops 20
Bpdu filter disabled globally
CIST regional root ID Priority 32768, Address 0001.e800.0204
CIST external path cost 0

Interface                             Designated
Name     PortID  Prio Cost Sts  Cost  Bridge ID         PortID
---------- -------- ---- ------- ----------- -------
--------------------
Te 0/41 128.170 128 2000   FWD  0   32768 0001.e800.0204
128.170
Te 0/42 128.171 128 2000   FWD  0   32768 0001.e800.0204
128.171
Te 0/43 128.172 128 2000   FWD  0   32768 0001.e800.0204
128.172

Interface Bpdu
```

```
Name    Role  PortID    Prio Cost Sts Cost Link-type Edge
Filter
Boundary
---------- ------ -------- ---- ------- ----------- -------
--------- ----
Te 0/41 Desg  128.170 128 2000   FWD  0    P2P      No    No
No
Te 0/42 Desg  128.171 128 2000   FWD  0    P2P      No    No
No
Te 0/43 Desg  128.172 128 2000   FWD  0    P2P      No    No
No
Dell#
```

Example (EDS and LBK)

The bold line shows the loopback BPDU inconsistency (LBK_INC).

```
Dell#show spanning-tree msti 0 brief
MSTI 0 VLANs mapped 1-4094

Executing IEEE compatible Spanning Tree Protocol
Root ID Priority 32768, Address 0001.e801.6aa8
Root Bridge hello time 2, max age 20, forward delay 15, max
hops 20
Bridge ID Priority 32768, Address 0001.e801.6aa8
We are the root of MSTI 0 (CIST)
Configured hello time 2, max age 20, forward delay 15, max
hops 20
CIST regional root ID Priority 32768, Address 0001.e801.6aa8
CIST external path cost 0

Interface                            Designated
Name    PortID   Prio Cost Sts Cost Bridge ID      PortID
----------------------------------------------------------
Gi 0/0  128.257  128  20000 EDS 0 32768 0001.e801.6aa8 128.257

Interface
Name  Role  PortID Prio Cost Sts Cost Link-type Edge Boundary
----------------------------------------------------------
Gi 0/0 ErrDis 128.257  128 20000 EDS 0   P2P       No   No

Dell#show spanning-tree msti 0
MSTI 0 VLANs mapped 1-4094

Root Identifier has priority 32768, Address 0001.e801.6aa8
Root Bridge hello time 2, max age 20, forward delay 15, max
hops 20
Bridge Identifier has priority 32768, Address 0001.e801.6aa8
Configured hello time 2, max age 20, forward delay 15, max
hops 20
We are the root of MSTI 0 (CIST)
Current root has priority 32768, Address 0001.e801.6aa8
CIST regional root ID Priority 32768, Address 0001.e801.6aa8
CIST external path cost 0
Number of topology changes 1, last change occured 00:00:15 ago
on Gi 0/0

Port 257 (GigabitEthernet 0/0) is LBK_INC Discarding
Port path cost 20000, Port priority 128, Port Identifier
128.257
Designated root has priority 32768, address 0001.e801.6aa8
Designated bridge has priority 32768, address 0001.e801.6aa8
Designated port id is 128.257, designated path cost 0
Number of transitions to forwarding state 1
```

```
BPDU (MRecords): sent 21, received 9
The port is not in the Edge port mode
```

Usage Information

The following describes the `show spanning-tree msti 5 guard` command shown in the following example.

Field	Description
Interface Name	MSTP interface.
Instance	MSTP instance.
Sts	Port state: root-inconsistent (INCON Root), forwarding (FWD), listening (LIS), blocking (BLK), or shut down (EDS Shut).
Guard Type	Type of STP guard configured (Root, Loop, or BPDU guard).

Example (Guard)

```
Dell#show spanning-tree msti 0 guard
Executing IEEE compatible Spanning Tree Protocol
Bpdu filter disabled globally

Interface
 Name     Instance Sts Guard type Bpdu Filter
--------- -------- --------- ---------- -----------
Te 0/41   0        FWD     None    No
Te 0/42   0        FWD     None    No
Te 0/43   0        FWD     None    No
```

spanning-tree

Enable the multiple spanning tree protocol on the interface.

Syntax

`spanning-tree`

To disable the multiple spanning tree protocol on the interface, use the `no spanning-tree` command.

Parameters

spanning-tree	Enter the keywords `spanning-tree` to enable the MSTP on the interface.

Defaults

Enable.

Command Modes

INTERFACE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

spanning-tree msti

Configure multiple spanning tree instance cost and priority for an interface.

Syntax

```
spanning-tree msti instance {cost cost | priority priority}
```

Parameters

msti *instance*	Enter the keyword `msti` and the MST instance number. The range is from zero (0) to 63.
cost *cost*	(OPTIONAL) Enter the keyword `cost` then the port cost value. The range is from 1 to 200000. The defaults are: • 40-Gigabit Ethernet interface = **1400** • 10-Gigabit Ethernet interface = **2000** • Port Channel interface with one 10 Gigabit Ethernet = **2000** • Port Channel with two 10 Gigabit Ethernet = **1800** • Port Channel with two 100 Mbps Ethernet = **180000**
priority *priority*	Enter keyword `priority` then a value in increments of 16 as the priority. The range is from 0 to 240. The default is **128**.

Defaults

- cost = depends on the interface type
- priority = **128**

Command Modes

INTERFACE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

spanning-tree mstp

Configures a Layer 2 MSTP interface as an edge port with (optionally) a bridge protocol data unit (BPDU) guard, or enables the root guard or loop guard feature on the interface.

Syntax

```
spanning-tree mstp {edge-port [bpduguard [shutdown-on-
violation]] | bpdufilter| rootguard}
```

Parameters

edge-port	Enter the keywords `edge-port` to configure the interface as a multiple spanning tree edge port.
bpduguard	(OPTIONAL) Enter the keyword `portfast` to enable Portfast to move the interface into forwarding mode immediately after the root fails. Enter the keyword `bpduguard` to disable the port when it receives a BPDU.

bpdufilter	(OPTIONAL) Enter the keyword `edgeport` to enable edge port configuration to move the interface into forwarding mode immediately after the root fails. Enter the keyword `bpdufilter` to stop sending and receiving BPDUs on the port-fast enabled ports.
shutdown-on-violation	(OPTIONAL) Enter the keywords `shutdown-on-violation` to hardware disable an interface when a BPDU is received and the port is disabled.
rootguard	Enter the keyword `rootguard` to enable root guard on an MSTP port or port-channel interface.

Command Modes

INTERFACE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

On an MSTP switch, a port configured as an edge port immediately transitions to the forwarding state. Only ports connected to end-hosts should be configured as an edge port. Consider an edge port similar to a port with `spanning-tree portfast` enabled.

Root guard and loop guard cannot be enabled at the same time on a port. For example, if you configure loop guard on a port on which root guard is already configured, the following error message is displayed: `% Error: RootGuard is configured. Cannot configure LoopGuard`.

When used in an MSTP network, if root guard blocks a boundary port in the CIST, the port is also blocked in all other MST instances.

Enabling Portfast BPDU guard and loop guard at the same time on a port results in a port that remains in a blocking state and prevents traffic from flowing through it. For example, when Portfast BPDU guard and loop guard are both configured:

- If a BPDU is received from a remote device, BPDU guard places the port in an err-disabled blocking state and no traffic is forwarded on the port.
- If no BPDU is received from a remote device, loop guard places the port in a loop-inconsistent blocking state and no traffic is forwarded on the port.

tc-flush-standard

Enable the MAC address flushing after receiving every topology change notification.

Syntax

`tc-flush-standard`

To disable, use the `no tc-flush-standard` command.

Defaults	Disabled.
Command Modes	CONFIGURATION
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	By default, the sytem implements an optimized flush mechanism for MSTP. This mechanism helps in flushing the MAC addresses only when necessary (and less often) allowing for faster convergence during topology changes. However, if a standards-based flush mechanism is needed, this `knob` command can be turned on to enable flushing MAC addresses after receiving every topology change notification.

35

Multicast

The multicast commands are supported by Dell Networking Operating System (OS).

This chapter contains the following sections:

- IPv4 Multicast Commands
- IPv6 Multicast Commands

IPv4 Multicast Commands

The following section contains the IPv4 multicast commands.

clear ip mroute

Clear learned multicast routes on the multicast forwarding table. To clear the protocol-independent multicast (PIM) tree information base, use the `clear ip pim tib` command.

Syntax	`clear ip mroute {`*`group-address`*` [`*`source-address`*`] | * | snooping}`
Parameters	*group-address [source-address]*: Enter the multicast group address and source address (if desired), in dotted decimal format, to clear information on a specific group. *: Enter * to clear all multicast routes. snooping: Enter the keyword `snooping` to delete multicast snooping route table entries.
Command Modes	EXEC Privilege
Command History	Version 9.2.(0.0): Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	show ip pim tib — shows the PIM tree information base.

ip mroute

Assign a static mroute.

Syntax

`ip mroute` *`destination mask`* `{`*`ip-address`*` | null 0| {{bgp| ospf}` *`process-id`*` | isis | rip | static} {`*`ip-address`*` | tag | null 0}} [distance]`

To delete a specific static mroute, use the `ip mroute` *`destination mask`* `{`*`ip-address`*` | null 0| {{bgp| ospf}` *`process-id`*` | isis | rip | static} {`*`ip-address`*` | tag | null 0}} [distance]` command.

To delete all mroutes matching a certain mroute, use the `no ip mroute` *`destination mask`* command.

Parameters

destination	Enter the IP address in dotted decimal format of the destination device.
mask	Enter the mask in slash prefix formation (/x) or in dotted decimal format.
null 0	(OPTIONAL) Enter the keyword `null` then zero (0).
[*protocol* [*process-id* | *tag*] *ip-address*]	(OPTIONAL) Enter one of the routing protocols: • Enter the BGP as-number then the IP address in dotted decimal format of the reverse path forwarding (RPF) neighbor. The range is from 1 to 65535. • Enter the OSPF process identification number then the IP address in dotted decimal format of the RPF neighbor. the range is from 1 to 65535. • Enter the IS-IS alphanumeric tag string then the IP address in dotted decimal format of the RPF neighbor. • Enter the RIP IP address in dotted decimal format of the RPF neighbor.
static *ip-address*	(OPTIONAL) Enter the Static IP address in dotted decimal format of the RPF neighbor.
ip-address	(OPTIONAL) Enter the IP address in dotted decimal format of the RPF neighbor.
distance	(OPTIONAL) Enter a number as the distance metric assigned to the mroute. The range is from 0 to 255.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands	show ip mroute — views the multicast routing table.

ip multicast-limit

To limit the number of multicast entries on the system, use this feature.

Syntax `ip multicast-limit *limit*`

Parameters

limit	Enter the desired maximum number of multicast entries on the system. The range is from 1 to 50000.

Defaults **15000** routes.

Command Modes CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

This feature allows you to limit the number of multicast entries on the system. This number is the total of all the multicast entries on all line cards in the system. On each line card, the multicast module only installs the maximum number of entries, depending on the configured CAM profile.

To store multicast routes, use the IN-L3-McastFib CAM partition. It is a separate hardware limit that exists per port-pipe. This hardware space limitation can supersede any software-configured limit. The opposite is also true, the CAM partition might not be exhausted at the time the system-wide route limit set by the `ip multicast-limit` command is reached.

ip multicast-routing

Enable IP multicast forwarding.

Syntax `ip multicast-routing`

To disable multicast forwarding, use the `no ip multicast-routing` command.

Defaults Disabled.

Command Modes CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

After you enable multicast, you can enable IGMP and PIM on an interface. In INTERFACE mode, enter the `ip pim sparse-mode` command to enable IGMP and PIM on the interface.

Related Commands

ip pim sparse-mode — enables IGMP and PIM on an interface.

show ip mroute

View the multicast routing table.

Syntax

```
show ip mroute [static | group-address [source-address] | count
| snooping [vlan vlan-id] [group-address [source-address]] |
summary | vlt [group-address [source-address] | count]
```

Parameters

static	(OPTIONAL) Enter the keyword `static` to view static multicast routes.
group-address [source-address]	(OPTIONAL) Enter the multicast group-address to view only routes associated with that group. Enter the source-address to view routes with that group-address and source-address.
count	(OPTIONAL) Enter the keyword `count` to view the number of multicast routes and packets.
snooping [vlan *vlan-id*] [*group-address* [*source-address*]]	Enter the keyword `snooping` to display information on the multicast routes PIM-SM snooping discovers. Enter a VLAN ID to limit the information displayed to the multicast routes PIM-SM snooping discovers on a specified VLAN. The VLAN ID range is from 1 to 4094. Enter a multicast group address and, optionally, a source multicast address in dotted decimal format (A.B.C.D) to limit the information displayed to the multicast routes PIM-SM snooping discovers for a specified multicast group and source.
summary	(OPTIONAL) Enter the keyword `summary` to view a summary of all routes.
vlt	(OPTIONAL) Enter the keyword `vlt` to view multicast routes with a spanned incoming interface. Enter a multicast group address in dotted decimal format (A.B.C.D) to limit the information displayed to the multicast routes for a specified multicast group and optionally a source multicast address in dotted decimal format (A.B.C.D) to limit the information

displayed for a specified multicast source. Enter the keyword `count` to display the total number of multicast routes with the spanned IIF.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2.(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Example (Static)

```
Dell#show ip mroute static

Mroute: 23.23.23.0/24, interface: Lo 2
Protocol: static, distance: 0, route-map: none, last change:
00:00:23
```

Example (Snooping)

```
Dell#show ip mroute snooping

IPv4 Multicast Snooping Table

(*, 224.0.0.0), uptime 17:46:23
  Incoming vlan: Vlan 2
  Outgoing interface list:
    GigabitEthernet 4/13

(*, 225.1.2.1), uptime 00:04:16
  Incoming vlan: Vlan 2
  Outgoing interface list:
    GigabitEthernet 4/11
    GigabitEthernet 4/13

(165.87.1.7, 225.1.2.1), uptime 00:03:17
  Incoming vlan: Vlan 2
  Outgoing interface list:
    GigabitEthernet 4/11
    GigabitEthernet 4/13
    GigabitEthernet 4/20
```

Example

```
Dell#show ip mroute

IP Multicast Routing Table

(*, 224.10.10.1), uptime 00:05:12
  Incoming interface: GigabitEthernet 3/12
  Outgoing interface list:
    GigabitEthernet 3/13

(1.13.1.100, 224.10.10.1), uptime 00:04:03
  Incoming interface: GigabitEthernet 3/4
  Outgoing interface list:
    GigabitEthernet 3/12
    GigabitEthernet 3/13

(*, 224.20.20.1), uptime 00:05:12
  Incoming interface: GigabitEthernet 3/12
  Outgoing interface list:
    GigabitEthernet 3/4
```

Usage Information

The following describes the `show ip mroute` command shown in the following example.

Field	Description
(S, G)	Displays the forwarding entry in the multicast route table.
uptime	Displays the amount of time the entry has been in the multicast forwarding table.
Incoming interface	Displays the reverse path forwarding (RPF) information towards the source for (S,G) entries and the RP for (*,G) entries.
Outgoing interface list:	Lists the interfaces that meet one of the following: • a directly connected member of the Group • statically configured member of the Group • received a (*,G) or (S,G) Join message

Example

```
Dell#show ip mroute

IP Multicast Routing Table

(*, 224.10.10.1), uptime 00:05:12
  Incoming interface: GigabitEthernet 3/12
  Outgoing interface list:
    GigabitEthernet 3/13

(1.13.1.100, 224.10.10.1), uptime 00:04:03
  Incoming interface: GigabitEthernet 3/4
  Outgoing interface list:
    GigabitEthernet 3/12
    GigabitEthernet 3/13

(*, 224.20.20.1), uptime 00:05:12
  Incoming interface: GigabitEthernet 3/12
  Outgoing interface list:
    GigabitEthernet 3/4
```

show ip rpf

View reverse path forwarding.

Syntax `show ip rpf`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)

Usage Information

Network administrators use static mroutes to control the reach-ability of the multicast sources. If a PIM-registered multicast source is reachable using static mroute as well as unicast route, the distance of each route is examined and the route with shorter distance is the one the PIM selects for reach-ability.

NOTE: The default distance of mroutes is zero (0) and is CLI configurable on a per route basis.

Example

```
Dell#show ip rpf
RPF information for 10.10.10.9
  RPF interface: Gi 3/4
  RPF neighbor: 165.87.31.4
  RPF route/mask: 10.10.10.9/255.255.255.255
  RPF type: unicast
```

IPv6 Multicast Commands

The following section contains the IPv6 multicast commands.

debug ipv6 mld_host

Enable the collection of debug information for MLD host transactions.

Syntax

`[no] debug ipv6 mld_host [`*`int-count`*` | `*`interface type`*`] [slot/port-range]`

To discontinue collection of debug information for the MLD host transactions, use the `no debug ipv6 mld_host` command.

Parameters

int-count — Enter the keyword `count` to indicate the number of required debug messages.

interface type — Enter the following keywords and slot/port information:

- For a 10G Ethernet interface, enter the keyword `tengigabitethernet` then the slot/port information.
- For a 40G interface, enter the keyword `fortyGigE` then the slot/port information.
- For a management interface, enter the keyword `managementinterface` then the slot/port information.
- For a port-channel interface, enter the keywords `port-channel` then the slot/port information.
- For a VLAN interface, enter the keyword `vlan` then the slot/port information.

Default

Disabled

Command Modes	EXEC
Command History	Version 9.2(0.0) — Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	To debug the MLD protocol for all ports or for specified ports, use the `debug ipv6 mld_host` command. Displayed information includes when a query is received, when a report is sent, when a mcast joins or leaves a group, and some reasons why an MLD query is rejected.

ip multicast-limit

To limit the number of multicast entries on the system, use this feature.

Syntax

`ip multicast-limit limit`

Parameters

limit	Enter the desired maximum number of multicast entries on the system. The range is from 1 to 50000.

Defaults

15000 routes.

Command Modes

CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

This feature allows you to limit the number of multicast entries on the system. This number is the total of all the multicast entries on all line cards in the system. On each line card, the multicast module only installs the maximum number of entries, depending on the configured CAM profile.

To store multicast routes, use the IN-L3-McastFib CAM partition. It is a separate hardware limit that exists per port-pipe. This hardware space limitation can supersede any software-configured limit. The opposite is also true, the CAM partition might not be exhausted at the time the system-wide route limit set by the `ip multicast-limit` command is reached.

36

Neighbor Discovery Protocol (NDP)

The Dell Networking Operating System (OS) supports the network discovery protocol for IPv6.

The neighbor discovery protocol for IPv6 is defined in RFC 2461 as part of the Stateless Address Autoconfiguration protocol. It replaces the Address Resolution Protocol used with IPv4. NDP defines mechanisms for solving the following problems:

- Router discovery: Hosts can locate routers residing on a link
- Prefix discovery: Hosts can discover address prefixes for the link
- Parameter discovery
- Address autoconfiguration — configuration of addresses for an interface
- Address resolution — mapping from IP address to link-layer address
- Next-hop determination
- Neighbor unreachability detection (NUD): Determine that a neighbor is no longer reachable on the link.
- Duplicate address detection (DAD): Allow a node to check whether a proposed address is already in use.
- Redirect: The router can inform a node about a better first-hop.

NDP uses the following five ICMPv6 packet types in its implementation:

- Router Solicitation
- Router Advertisement
- Neighbor Solicitation
- Neighbor Advertisement
- Redirect

clear ipv6 neighbors

Delete all entries in the IPv6 neighbor discovery cache or neighbors of a specific interface. Static entries are not removed using this command.

Syntax `clear ipv6 neighbors [`*`ipv6-address`*`] [`*`interface`*`]`

Parameters

ipv6-address	Enter the IPv6 address of the neighbor in the x:x:x:x::x format to remove a specific IPv6 neighbor. **NOTE:** The :: notation specifies successive hexadecimal fields of zero.
interface *interface*	To remove all neighbor entries learned on a specific interface, enter the keyword `interface` then the interface type and slot/port or number information of the interface:

- For a Fast Ethernet interface, enter the keyword `fastEthernet` then the slot/port information.
- For a Port Channel interface, enter the keywords `port-channel` then a number.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a VLAN, enter the keyword `vlan` then the VLAN ID. The range is from 1 to 4094.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

ipv6 neighbor

Configure a static entry in the IPv6 neighbor discovery.

Syntax

`ipv6 neighbor {`*`ipv6-address`*`} {interface `*`interface`*`} {`*`hardware_address`*`}`

To remove a static IPv6 entry from the IPv6 neighbor discovery, use the `no ipv6 neighbor {`*`ipv6-address`*`} {interface `*`interface`*`}` command.

Parameters

ipv6-address	Enter the IPv6 address of the neighbor in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zero.
interface *interface*	Enter the keyword `interface` then the interface type and slot/port or number information: • For a Fast Ethernet interface, enter the keyword `fastEthernet` then the slot/port information. • For a Port Channel interface, enter the keywords `port-channel` then a number. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

hardware_address	Enter a 48-bit hardware MAC address in nn:nn:nn:nn:nn:nn format.

Defaults none

Command Modes CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

show ipv6 neighbors

Display IPv6 discovery information. Entering the command without options shows all IPv6 neighbor addresses stored on the control processor (CP).

Syntax

```
show ipv6 neighbors [ipv6-address] [cpu {rp1 [ipv6-address] |
rp2 [ipv6-address]}}] [interface interface]
```

Parameters

ipv6-address	Enter the IPv6 address of the neighbor in the x:x:x:x::x format. NOTE: The :: notation specifies successive hexadecimal fields of zero.
CPU	Enter the keyword `cpu` then either `rp1` or `rp2` (Route Processor 1 or 2), optionally then an IPv6 address to display the IPv6 neighbor entries stored on the designated RP.
interface *interface*	Enter the keyword `interface` then the interface type and slot/port or number information: • For a Fast Ethernet interface, enter the keyword `fastEthernet` then the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a VLAN, enter the keyword `vlan` then the VLAN ID. The range is from 1 to 4094.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#   show ipv6 neighbors
IPv6 Address                Expires(min)   Hardware
Address      State       Interface    VLAN      CPU
---------------------------------------------------------------
--------------------------------------------------------
100::1                         0.03
00:00:00:00:00:22    DELAY       Te 0/12        -       CP
fe80::200:ff:fe00:22          232
00:00:00:00:00:22    STALE       Te 0/12        -       CP
500::1                         0.60
00:01:e8:17:5c:af    REACH       Te 0/13        -       CP
fe80::200:ff:fe00:17          232
00:00:00:00:00:29    REACH       Te 0/14        -       CP
900::1                         0.60
00:01:e8:17:5c:b1    STALE       Po 23          -       CP
400::1                         0.60
00:01:e8:17:5c:ae    REACH       te 0/2         Vl      100 CP
Dell#
```

37

Open Shortest Path First (OSPFv2 and OSPFv3)

The MXL 10/40GbE Switch IO Module platform supports open shortest path first version 2 (OSPFv2) for IPv4 and version 3 (OSPFv3) for IPv6. Up to 16 OSPF instances can be run simultaneously on the MXL Switch.

OSPF is an Interior Gateway Protocol (IGP), which means that it distributes routing information between routers in a single Autonomous System (AS). OSPF is also a link-state protocol in which all routers contain forwarding tables derived from information about their links to their neighbors.

The fundamental mechanisms of OSPF (flooding, DR election, area support, SPF calculations, and so on) are the same for OSPFv2 and OSPFv3. OSPFv3 runs on a per-link basis instead of on a per-IP-subnet basis.

This chapter is divided into two sections. There is no overlap between the two sets of commands. You cannot use an OSPFv2 command in the IPv6 OSPFv3 mode.

- OSPFv2 Commands
- OSPFv3 Commands

NOTE:
Multi-process OSPF is supported on IPV4 OSPFv2 only. It is not supported on IPv6 OSPFv3.

The CLI requires that you include the Process ID when entering ROUTER-OSPF mode. Each command entered applies to the specified OSPFv2 process only.

OSPFv2 Commands

The Dell Networking implementation of OSPFv2 is based on IETF RFC 2328.

area default-cost

Set the metric for the summary default route the area border router (ABR) generates into the stub area. Use this command on the border routers at the edge of a stub area.

Syntax	`area area-id default-cost cost` To return default values, use the `no area area-id default-cost` command.

Parameters

area-id	Specify the OSPF area in dotted decimal format (A.B.C.D.) or enter a number from zero (0) to 65535.
cost	Specifies the stub area's advertised external route metric. The range is from zero (0) to 65535.

Defaults *cost* = **1**; no areas are configured.

Command Modes ROUTER OSPF

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information In the Dell Networking operating software, `cost` is defined as reference bandwidth.

Related Commands area stub — creates a stub area.

area nssa

Specify an area as a not so stubby area (NSSA).

Syntax

```
area area-id nssa [default-information-originate] [no-redistribution] [no-summary]
```

To delete an NSSA, use the `no area area-id nssa` command.

Parameters

area-id	Specify the OSPF area in dotted decimal format (A.B.C.D.) or enter a number from zero (0) to 65535.
no-redistribution	(OPTIONAL) Specify that the `redistribute` command does not distribute routes into the NSSA. Only use this command in an NSSA area border router (ABR).
default-information-originate	(OPTIONAL) Allows external routing information to be imported into the NSSA by using Type 7 default.
no-summary	(OPTIONAL) Specify that no summary LSAs should be sent into the NSSA.

Defaults Not configured.

Command Modes ROUTER OSPF

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

area range

Summarize routes matching an address/mask at an area border router (ABR).

Syntax

`area area-id range ip-address mask [not-advertise]`

To disable route summarization, use the `no area area-id range ip-address mask` command.

Parameters

area-id	Specify the OSPF area in dotted decimal format (A.B.C.D.) or enter a number from zero (0) to 65535.
ip-address	Specify an IP address in dotted decimal format.
mask	Specify a mask for the destination prefix. Enter the full mask (for example, 255.255.255.0).
not-advertise	(OPTIONAL) Enter the keywords `not-advertise` to set the status to DoNotAdvertise (that is, the Type 3 summary-LSA is suppressed and the component networks remain hidden from other areas.)

Defaults

Not configured.

Command Modes

ROUTER OSPF

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Only the routes within an area are summarized, and that summary is advertised to other areas by the ABR. External routes are not summarized.

Related Commands

area stub — creates a stub area.

router ospf — enters ROUTER OSPF mode to configure an OSPF instance.

area stub

Configure a stub area, which is an area not connected to other areas.

Syntax

`area area-id stub [no-summary]`

To delete a stub area, use the `no area area-id stub` command.

Parameters

area-id	Specify the OSPF area in dotted decimal format (A.B.C.D.) or enter a number from zero (0) to 65535.
no-summary	(OPTIONAL) Enter the keywords `no-summary` to prevent the ABR from sending summary Link State Advertisements (LSAs) into the stub area.

Defaults	Disabled.
Command Modes	ROUTER OSPF
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	To configure all routers and access servers within a stub, use this command.
Related Commands	router ospf — enters ROUTER OSPF mode to configure an OSPF instance.

auto-cost

Specify how the OSPF interface cost is calculated based on the reference bandwidth method.

Syntax

`auto-cost [reference-bandwidth ref-bw]`

To return to the default bandwidth or to assign cost based on the interface type, use the `no auto-cost [reference-bandwidth]` command.

Parameters

ref-bw	(OPTIONAL) Specify a reference bandwidth in megabits per second. The range is from 1 to 4294967. The default is **100 megabits per second**.

Defaults	**100 megabits per second**.
Command Modes	ROUTER OSPF
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

clear ip ospf

Clear all OSPF routing tables.

Syntax

`clear ip ospf process-id [process]`

Parameters

process-id	Enter the OSPF Process ID to clear a specific process. If no Process ID is entered, all OSPF processes are cleared.
process	(OPTIONAL) Enter the keyword `process` to reset the OSPF process.

Command Modes	EXEC Privilege	
Command History	**Version 8.3.16.1**	Introduced on the MXL 10/40GbE Switch IO Module.

clear ip ospf statistics

Clear the packet statistics in interfaces and neighbors.

Syntax

`clear ip ospf process-id statistics [interface name {neighbor router-id}]`

Parameters

process-id	Enter the OSPF Process ID to clear a specific process. If no Process ID is entered, all OSPF processes are cleared.
interface *name*	(OPTIONAL) Enter the keyword `interface` then one of the following interface keywords and slot/port or number information: • For Port Channel groups, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a VLAN, enter the keyword `vlan` then a number from 1 to 4094. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
neighbor *router-id*	(OPTIONAL) Enter the keyword `neighbor` then the neighbor's router-id in dotted decimal format (A.B.C.D.).

Defaults	none	
Command Modes	EXEC Privilege	
Command History	**Version 8.3.16.1**	Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	show ip ospf statistics — displays the OSPF statistics.	

debug ip ospf

Display debug information on OSPF. Entering the `debug ip ospf` commands enables OSPF debugging for the first OSPF process.

Syntax

`debug ip ospf` *`process-id`* `[bfd |event | packet | spf | database-timer rate-limit]`

To cancel the debug command, use the `no debug ip ospf` command.

Parameters

process-id	Enter the OSPF Process ID to clear a specific process. If no Process ID is entered, all OSPF processes are cleared.
bfd	(OPTIONAL) Enter the keyword `bfd` to debug only OSPF BFD information.
event	(OPTIONAL) Enter the keyword `event` to debug only OSPF event information.
packet	(OPTIONAL) Enter the keyword `packet` to debug only OSPF packet information.
spf	(OPTIONAL) Enter the keyword `spf` to display the Shortest Path First information.
database-timer rate-limit	(OPTIONAL) Enter the keywords `database-timer rate-limit` to display the LSA throttling timer information.

Command Modes

EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `debug ip ospf` command shown in the Example below.

Field	Description
8:14	Displays the time stamp.
OSPF	Displays the OSPF process ID: instance ID.
v:	Displays the OSPF version. The system supports version 2 only.
t:	Displays the type of packet sent: • 1 - Hello packet • 2 - database description • 3 - link state request • 4 - link state update • 5 - link state acknowledgement
l:	Displays the packet length.

Field	Description
rid:	Displays the OSPF router ID.
aid:	Displays the Autonomous System ID.
chk:	Displays the OSPF checksum.
aut:	States if OSPF authentication is configured. One of the following is listed: • 0 - no authentication configured • 1 - simple authentication configured using the `ip ospf authentication-key` command • 2 - MD5 authentication configured using the `ip ospf message-digest-key` command
auk:	If the `ip ospf authentication-key` command is configured, this field displays the key used.
keyid:	If the `ip ospf message-digest-key` command is configured, this field displays the MD5 key
to:	Displays the interface to which the packet is intended.
dst:	Displays the destination IP address.
netmask:	Displays the destination IP address mask.
pri:	Displays the OSPF priority
N, MC, E, T	Displays information available in the Options field of the HELLO packet: • N + (N-bit is set) • N - (N-bit is not set) • MC+ (bit used by MOSPF is set and router is able to forward IP multicast packets) • MC- (bit used by MOSPF is not set and router cannot forward IP multicast packets) • E + (router is able to accept AS External LSAs) • E - (router cannot accept AS External LSAs) • T + (router can support TOS) • T - (router cannot support TOS)
hi:	Displays the amount of time configured for the HELLO interval.
di:	Displays the amount of time configured for the DEAD interval.
dr:	Displays the IP address of the designated router.
bdr:	Displays the IP address of the Border Area Router.

Example

```
Dell#debug ip ospf 1 packet
OSPF process 90, packet debugging is on

Dell#
08:14:24 : OSPF(100:00):
Xmt. v:2 t:1(HELLO) l:44 rid:192.1.1.1
   aid:0.0.0.1 chk:0xa098 aut:0 auk: keyid:0 to:Gi 4/3 dst:
224.0.0.5
      netmask:255.255.255.0 pri:1 N-, MC-, E+, T-,
      hi:10 di:40 dr:90.1.1.1 bdr:0.0.0.0
```

default-information originate

To generate a default external route into an OSPF routing domain, configure the system.

Syntax

`default-information originate [always] [metric metric-value] [metric-type type-value] [route-map map-name]`

To return to the default values, use the `no default-information originate` command.

Parameters

always	(OPTIONAL) Enter the keyword `always` to specify that default route information must always be advertised.
metric *metric-value*	(OPTIONAL) Enter the keyword `metric` then a number to configure a metric value for the route. The range is from 1 to 16777214.
metric-type *type-value*	(OPTIONAL) Enter the keywords `metric-type` then an OSPF link state type of 1 or 2 for default routes. The values are: • 1 = Type 1 external route • 2 = Type 2 external route
route-map *map-name*	(OPTIONAL) Enter the keywords `route-map` then the name of an established route map.

Defaults

Disabled.

Command Modes

ROUTER OSPF

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

redistribute — redistributes routes from other routing protocols into OSPF.

default-metric

Change the metrics of redistributed routes to a value useful to OSPF. Use this command with the `redistribute` command.

Syntax	`default-metric number` To return to the default values, use the `no default-metric [number]` command.
Parameters	***number*** — Enter a number as the metric. The range is from 1 to 16777214.
Defaults	Disabled.
Command Modes	ROUTER OSPF
Command History	**Version 8.3.16.1** — Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	redistribute — redistributes routes from other routing protocols into OSPF.

description

Add a description about the selected OSPF configuration.

Syntax	`description description` To remove the OSPF description, use the `no description` command.
Parameters	***description*** — Enter a text string description to identify the OSPF configuration (80 characters maximum).
Defaults	none
Command Modes	ROUTER OSPF
Command History	**Version 8.3.16.1** — Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	show ip ospf asbr — displays the VLAN configuration.

distance

Define an administrative distance for particular routes to a specific IP address.

Syntax

`distance weight [ip-address mask access-list-name]`

To delete the settings, use the `no distance weight [ip-address mask access-list-name]` command.

Parameters

weight	Specify an administrative distance. The range is from 1 to 255. The default is **110**.
ip-address	(OPTIONAL) Enter a router ID in the dotted decimal format. If you enter a router ID, include the mask for that router address.
mask	(OPTIONAL) Enter a mask in dotted decimal format or /n format.
access-list-name	(OPTIONAL) Enter the name of an IP standard access list, up to 140 characters.

Defaults **110**

Command Modes ROUTER OSPF

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

distance ospf

Configure an OSPF distance metric for different types of routes.

Syntax

`distance ospf [external dist3] [inter-area dist2] [intra-area dist1]`

To delete these settings, use the `no distance ospf` command.

Parameters

external *dist3*	(OPTIONAL) Enter the keyword `external` then a number to specify a distance for external type 5 and 7 routes. The range is from 1 to 255. The default is **110**.
inter-area *dist2*	(OPTIONAL) Enter the keywords `inter-area` then a number to specify a distance metric for routes between areas. The range is from 1 to 255. The default is **110**.
intra-area *dist1*	(OPTIONAL) Enter the keywords `intra-area` then a number to specify a distance metric for all routes within an area. The range is from 1 to 255. The default is **110**.

Defaults	- external *dist3* = **110** - inter-area *dist2* = **110** - intra-area *dist1* = **110**
Command Modes	ROUTER OSPF
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	To specify a distance for routes learned from other routing domains, use the `redistribute` command.

distribute-list in

Apply a filter to incoming routing updates from OSPF to the routing table.

Syntax

`distribute-list prefix-list-name in [interface]`

To delete a filter, use the `no distribute-list prefix-list-name in [interface]` command.

Parameters

prefix-list-name	Enter the name of a configured prefix list.
interface	(OPTIONAL) Enter one of the following keywords and slot/port or number information: - For Port Channel groups, enter the keywords `port-channel` then a number. The range is from 1 to 128. - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. - For a VLAN, enter the keyword `vlan` then a number from 1 to 4094. - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

Defaults	Not configured.
Command Modes	ROUTER OSPF
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

distribute-list out

To restrict certain routes destined for the local routing table after the SPF calculation, apply a filter.

Syntax

`distribute-list *prefix-list-name* out [bgp | connected | isis | rip | static]`

To remove a filter, use the `no distribute-list *prefix-list-name* out [bgp | connected | isis | rip | static]` command.

Parameters

prefix-list-name	Enter the name of a configured prefix list.
bgp	(OPTIONAL) Enter the keyword `bgp` to specify that BGP routes are distributed.
connected	(OPTIONAL) Enter the keyword `connected` to specify that connected routes are distributed.
isis	(OPTIONAL) Enter the keyword `isis` to specify that IS-IS routes are distributed.
rip	(OPTIONAL) Enter the keyword `rip` to specify that RIP routes are distributed.
static	(OPTIONAL) Enter the keyword `static` to specify that only manually configured routes are distributed.

Defaults

Not configured.

Command Modes

ROUTER OSPF

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The `distribute-list out` command applies to routes autonomous system boundary routers (ASBRs) redistributes into OSPF. It can be applied to external type 2 and external type 1 routes, but not to intra-area and inter-area routes.

fast-convergence

This command sets the minimum LSA origination and arrival times to zero (0), allowing more rapid route computation so that convergence takes less time.

Syntax

`fast-convergence {*number*}`

To cancel fast-convergence, use the `no fast convergence` command.

Parameters

number	Enter the convergence level desired. The higher this parameter is set, the faster OSPF converge takes place. The range is from 1 to 4.

Defaults none.

Command Modes ROUTER OSPF

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The higher this parameter is set, the faster OSPF converge takes place.

NOTE: The faster the convergence, the more frequent the route calculations and updates. This behavior impacts CPU utilization and may impact adjacency stability in larger topologies.

Generally, convergence level 1 meets most convergence requirements. Higher convergence levels should only be selected following consultation with Dell Networking technical support.

flood-2328

Enable RFC-2328 flooding behavior.

Syntax `flood-2328`

To disable, use the `no flood-2328` command.

Defaults Disabled.

Command Modes ROUTER OSPF

Command History

Version 8.3.16.1	

Usage Information

In OSPF, flooding is the most resource-consuming task. The flooding algorithm, described in RFC-2328, requires that OSPF flood LSAs (Link State Advertisements) on all interfaces, as governed by LSA's flooding scope (see Section 13 of the RFC). When multiple direct links connect two routers, the RFC-2328 flooding algorithm generates significant redundant information across all links.

By default, the system implements an enhanced flooding procedure that dynamically and intelligently determines when to optimize flooding. Whenever possible, the OSPF task attempts to reduce flooding overhead by selectively flooding on a subset of the interfaces between two routers.

When you enable `flood-2328`, this command configures the system to flood LSAs on all interfaces.

graceful-restart grace-period

Specifies the time duration, in seconds, that the router's neighbors continue to advertise the router as fully adjacent regardless of the synchronization state during a graceful restart.

Syntax	`graceful-restart grace-period` *`seconds`* To disable the grace period, use the `no graceful-restart grace-period` command.
Parameters	
	seconds — Time duration, in seconds, that specifies the duration of the restart process before OSPF terminates the process. The range is from 40 to 1800 seconds.
Defaults	Not Configured
Command Modes	ROUTER OSPF
Command History	**Version 8.3.16.1** — Introduced on the MXL 10/40GbE Switch IO Module.

graceful-restart helper-reject

Specify the OSPF router to not act as a helper during graceful restart.

Syntax	`graceful-restart helper-reject` *`ip-address`* To return to default value, use the `no graceful-restart helper-reject` command.
Parameters	
	ip-address — Enter the OSPF router-id, in IP address format, of the restart router that *will not* act as a helper during graceful restart.
Defaults	Not configured.
Command Modes	ROUTER OSPF
Command History	**Version 8.3.16.1** — Introduced on the MXL 10/40GbE Switch IO Module.

graceful-restart mode

Enable the graceful restart mode.

Syntax	`graceful-restart mode [planned-only | unplanned-only]` To disable graceful restart mode, use the `no graceful-restart mode` command.
Parameters	**planned-only**: (OPTIONAL) Enter the keywords `planned-only` to indicate graceful restart is supported in a planned restart condition only. **unplanned-only**: (OPTIONAL) Enter the keywords `unplanned-only` to indicate graceful restart is supported in an unplanned restart condition only.
Defaults	Support for both planned and unplanned failures.
Command Modes	ROUTER OSPF
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

graceful-restart role

Specify the role for your OSPF router during graceful restart.

Syntax	`graceful-restart role [helper-only | restart-only]` To disable graceful restart role, use the `no graceful-restart role` command.
Parameters	**role helper-only**: (OPTIONAL) Enter the keywords `helper-only` to specify the OSPF router is a helper only during graceful restart. **role restart-only**: (OPTIONAL) Enter the keywords `restart-only` to specify the OSPF router is a restart only during graceful-restart.
Defaults	By default, OSPF routers are both helper and restart routers during a graceful restart.
Command Modes	ROUTER OSPF
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

ip ospf auth-change-wait-time

OSPF provides a grace period while OSPF changes its interface authentication type. During the grace period, OSPF sends out packets with new and old authentication scheme until the grace period expires.

Syntax

```
ip ospf auth-change-wait-time seconds
```

To return to the default, use the `no ip ospf auth-change-wait-time` command.

Parameters

seconds	Enter the seconds. The range is from 0 to 300.

Defaults

zero (0) seconds.

Command Modes

INTERFACE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

ip ospf authentication-key

Enable authentication and set an authentication key on OSPF traffic on an interface.

Syntax

```
ip ospf authentication-key [encryption-type] key
```

To delete an authentication key, use the `no ip ospf authentication-key` command.

Parameters

encryption-type	(OPTIONAL) Enter 7 to encrypt the key.
key	Enter an eight-character string. Strings longer than eight characters are truncated.

Defaults

Not configured.

Command Modes

INTERFACE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

All neighboring routers in the same network must use the same password to exchange OSPF information.

ip ospf cost

Change the cost associated with the OSPF traffic on an interface.

Syntax

`ip ospf cost cost`

To return to default value, use the `no ip ospf cost` command.

Parameters

cost	Enter a number as the cost. The range is from 1 to 65535.

Defaults

The default cost is based on the reference bandwidth.

Command Modes

INTERFACE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

If this command is not configured, cost is based on the `auto-cost` command.

When you configure OSPF over multiple vendors, to ensure that all routers use the same cost, use the `ip ospf cost` command. Otherwise, OSPF routes improperly.

Related Commands

auto-cost — controls how the OSPF interface cost is calculated.

ip ospf dead-interval

Set the time interval since the last hello-packet was received from a router. After the interval elapses, the neighboring routers declare the router dead.

Syntax

`ip ospf dead-interval seconds`

To return to the default values, use the `no ip ospf dead-interval` command.

Parameters

seconds	Enter the number of seconds for the interval. The range is from 1 to 65535. The default is **40 seconds**.

Defaults

40 seconds

Command Modes

INTERFACE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

By default, the dead interval is four times the default hello-interval.

Related Commands	ip ospf hello-interval — sets the time interval between the hello packets.

ip ospf hello-interval

Specify the time interval between the hello packets sent on the interface.

Syntax

```
ip ospf hello-interval seconds
```

To return to the default value, use the `no ip ospf hello-interval` command.

Parameters

seconds	Enter the number of seconds for the interval. The range is from 1 to 65535. The default is **10 seconds**.

Defaults	**10 seconds**
Command Modes	INTERFACE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information	The time interval between the hello packets must be the same for routers in a network.
Related Commands	ip ospf dead-interval — sets the time interval before a router is declared dead.

ip ospf message-digest-key

Enable OSPF MD5 authentication and send an OSPF message digest key on the interface.

Syntax

```
ip ospf message-digest-key keyid md5key
```

To delete a key, use the `no ip ospf message-digest-key keyid` command.

Parameters

keyid	Enter a number as the key ID. The range is from 1 to 255.
key	Enter a continuous character string as the password.

Defaults	No MD5 authentication is configured.
Command Modes	INTERFACE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

You can configure a maximum of six digest keys on an interface. Of the available six digest keys, the switches select the MD5 key that is common. The remaining MD5 keys are unused.

To change to a different key on the interface, enable the new key while the old key is still enabled. The system sends two packets: the first packet authenticated with the old key and the second packet authenticated with the new key. This process ensures that the neighbors learn the new key and communication is not disrupted by keeping the old key enabled.

After the reply is received and the new key is authenticated, delete the old key. Dell recommends keeping only one key per interface.

NOTE: The MD5 secret is stored as plain text in the configuration file with service password encryption. Write down or otherwise record the key. You cannot learn the key once it is configured. Use caution when changing the key.

ip ospf mtu-ignore

Disable OSPF MTU mismatch detection upon receipt of database description (DBD) packets.

Syntax

```
ip ospf mtu-ignore
```

To return to the default, use the `no ip ospf mtu-ignore` command.

Defaults

Enabled.

Command Modes

INTERFACE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

ip ospf network

Set the network type for the interface.

Syntax

```
ip ospf network {broadcast | point-to-point}
```

To return to the default, use the `no ip ospf network` command.

Parameters

broadcast	Enter the keyword `broadcast` to designate the interface as part of a broadcast network.
point-to-point	Enter the keywords `point-to-point` to designate the interface as part of a point-to-point network.

Defaults	Not configured.
Command Modes	ROUTER OSPF
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

ip ospf priority

To determine the designated router for the OSPF network, set the priority of the interface.

Syntax

`ip ospf priority number`

To return to the default setting, use the `no ip ospf priority` command.

Parameters

number	Enter a number as the priority. The range is from 0 to 255. The default is **1**.

Defaults **1**

Command Modes INTERFACE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Setting a priority of 0 makes the router ineligible for election as a designated router or backup designated router.

Use this command for interfaces connected to multi-access networks, not point-to-point networks.

ip ospf retransmit-interval

Set the retransmission time between lost link state advertisements (LSAs) for adjacencies belonging to the interface.

Syntax

`ip ospf retransmit-interval seconds`

To return to the default values, use the `no ip ospf retransmit-interval` command.

Parameters

seconds	Enter the number of seconds as the interval between retransmission. The range is from 1 to 3600. The default is **5 seconds**.

This interval must be greater than the expected round-trip time for a packet to travel between two routers.

Defaults	**5 seconds**
Command Modes	INTERFACE
Command History	Version 8.3.16.1 — Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	Set the time interval to a number large enough to prevent unnecessary retransmissions. For example, the interval must be larger for interfaces connected to virtual links.

ip ospf transmit-delay

To send a link state update packet on the interface, set the estimated time elapsed.

Syntax

```
ip ospf transmit-delay seconds
```

To return to the default value, use the `no ip ospf transmit-delay` command.

Parameters

seconds	Enter the number of seconds as the interval between retransmission. The range is from 1 to 3600. The default is **1 second**. This value must be greater than the transmission and propagation delays for the interface.

Defaults	**1 second**
Command Modes	INTERFACE
Command History	Version 8.3.16.1 — Introduced on the MXL 10/40GbE Switch IO Module.

log-adjacency-changes

To send a Syslog message about changes in the OSPF adjacency state, set the system.

Syntax

```
log-adjacency-changes
```

To disable the Syslog messages, use the `no log-adjacency-changes` command.

Defaults	Disabled.
Command Modes	ROUTER OSPF
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

maximum-paths

Enable the software to forward packets over multiple paths.

Syntax `maximum-paths *number*`

To disable packet forwarding over multiple paths, use the `no maximum-paths` command.

Parameters

number	Specify the number of paths. The range for OSPFv2 is from 1 to 16. The default for OSPFv2 is **4 paths**. The range for OSPFv3 is from 1 to 64. The default for OSPFv3 is **8 paths**.

Defaults **4**

Command Modes

ROUTER OSPF for OSPFv2

ROUTER OSPFv3 for OSPFv3

Command History

Version 9.2(0.0)	Added support for OSPFv3.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

mib-binding

Enable this OSPF process ID to manage the SNMP traps and process SNMP queries.

Syntax `mib-binding`

To mib-binding on this OSPF process, use the `no mib-binding` command.

Defaults	none.
Command Modes	ROUTER OSPF
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

This command is either enabled or disabled. If no OSPF process is identified as the MIB manager, the first OSPF process is used.

If an OSPF process has been selected, it must be disabled prior to assigning new process ID the MIB responsibility.

network area

Define which interfaces run OSPF and the OSPF area for those interfaces.

Syntax

`network ip-address mask area area-id`

To disable an OSPF area, use the `no network ip-address mask area area-id` command.

Parameters

ip-address	Specify a primary or secondary address in dotted decimal format. The primary address is required before adding the secondary address.
mask	Enter a network mask in /prefix format. (/x)
area-id	Enter the OSPF area ID as either a decimal value or in a valid IP address. Decimal value range is from 0 to 65535. IP address format is dotted decimal format A.B.C.D. **NOTE:** If the area ID is smaller than 65535, it is converted to a decimal value. For example, if you use an area ID of 0.0.0.1, it is converted to 1.

Command Modes

ROUTER OSPF

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To enable OSPF on an interface, the `network area` command must include, in its range of addresses, the primary IP address of an interface.

NOTE: An interface can be attached only to a single OSPF area.

If you delete all the network area commands for Area 0, the `show ip ospf` command output does not list Area 0.

passive-interface

Suppress both receiving and sending routing updates on an interface.

Syntax	`passive-interface {default	interface}` To enable both the receiving and sending routing, use the `no passive-interface interface` command. To return all OSPF interfaces (current and future) to active, use the `no passive-interface default` command.

Parameters

default	Enter the keyword `default` to make all OSPF interfaces (current and future) passive.
interface	Enter the following keywords and slot/port or number information: • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For Port Channel groups, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

Command Modes ROUTER OSPF

Command History

Version 8.3.19.0	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Although the passive interface does not send or receive routing updates, the network on that interface is still included in OSPF updates sent using other interfaces.

The `default` keyword sets all interfaces as passive. You can then configure individual interfaces, where adjacencies are desired, using the `no passive-interface interface` command. The `no` form of this command is inserted into the configuration for individual interfaces when the `no passive-interface interface` command is issued while `passive-interface default` is configured.

This command behavior has changed as follows:

`passive-interface interface`

- The previous `no passive-interface interface` is removed from the running configuration.

- The ABR status for the router is updated.
- Save `passive-interface` *`interface`* into the running configuration.

`passive-interface default`

- All present and future OSPF interfaces are marked as *passive*.
- Any adjacency is explicitly terminated from all OSPF interfaces.
- All previous `passive-interface` *`interface`* commands are removed from the running configuration.
- All previous `no passive-interface` *`interface`* commands are removed from the running configuration.

`no passive-interface` *`interface`*

- Remove the interface from the passive list.
- The ABR status for the router is updated.
- If `passive-interface default` is specified, then save `no passive-interface` *`interface`* into the running configuration.

`No passive-interface default`

- Clear everything and revert to the default behavior.
- All previously marked passive interfaces are removed.
- May update ABR status.

redistribute

Redistribute information from another routing protocol throughout the OSPF process.

Syntax

`redistribute {connected | rip | static} [metric` *`metric-value`* `| metric-type` *`type-value`*`] [route-map` *`map-name`*`] [tag` *`tag-value`*`]`

To disable redistribution, use the `no redistribute {connected | isis | rip | static}` command.

Parameters

connected	Enter the keyword `connected` to specify that information from active routes on interfaces is redistributed.
rip	Enter the keyword `rip` to specify that RIP routing information is redistributed.
static	Enter the keyword `static` to specify that information from static routes is redistributed.
metric *metric-value*	(OPTIONAL) Enter the keyword `metric` then a number. The range is from 0 (zero) to 16777214.
metric-type *type-value*	(OPTIONAL) Enter the keywords `metric-type` then one of the following:

- 1 = OSPF External type 1
- 2 = OSPF External type 2

route-map *map-name*	(OPTIONAL) Enter the keywords `route-map` then the name of the route map.
tag *tag-value*	(OPTIONAL) Enter the keyword `tag` then a number. The range is from 0 to 4294967295.

Defaults Not configured.

Command Modes ROUTER OSPF

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information To redistribute the default route (0.0.0.0/0), configure the `default-information originate` command.

Related Commands default-information originate — generates a default route into the OSPF routing domain.

redistribute bgp

Redistribute BGP routing information throughout the OSPF instance.

Syntax `redistribute bgp as` *`number`* `[metric` *`metric-value`*`] | [metric-type` *`type-value`*`] | [tag` *`tag-value`*`]`

To disable redistribution, use the `no redistribute bgp as` *`number`* `[metric` *`metric-value`*`] | [metric-type` *`type-value`*`] [tag` *`tag-value`*`]` command.

Parameters

as number	Enter the autonomous system number. The range is from 1 to 65535.
metric *metric-value*	(OPTIONAL) Enter the keyword `metric` then the metric-value number. The range is from 0 to16777214.
metric-type *type-value*	(OPTIONAL) Enter the keywords `metric-type` then one of the following: • 1 = for OSPF External type 1 • 2 = for OSPF External type 2
tag *tag-value*	(OPTIONAL) Enter the keyword `tag` to set the tag for routes redistributed into OSPF. The range is from 0 to 4294967295.

Defaults none

Command Modes	ROUTER OSPF
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

redistribute isis

Redistribute IS-IS routing information throughout the OSPF instance.

Syntax

`redistribute isis [`*`tag`*`] [level-1 | level-1-2 | level-2] [metric `*`metric-value`*` | metric-type `*`type-value`*`] [route-map `*`map-name`*`] [tag `*`tag-value`*`]`

To disable redistribution, use the `no redistribute isis [`*`tag`*`] [level-1 | level-1-2 | level-2] [metric `*`metric-value`*` | metric-type `*`type-value`*`] [route-map `*`map-name`*`] [tag `*`tag-value`*`]` command.

Parameters

tag	(OPTIONAL) Enter the name of the IS-IS routing process.
level-1	(OPTIONAL) Enter the keywords `level-1` to redistribute only IS-IS Level-1 routes.
level-1-2	(OPTIONAL) Enter the keywords `level-1-2` to redistribute both IS-IS Level-1 and Level-2 routes.
level-2	(OPTIONAL) Enter the keywords `level-2` to redistribute only IS-IS Level-2 routes.
metric *metric-value*	(OPTIONAL) Enter the keyword `metric` then a number. The range is from 0 (zero) to 4294967295.
metric-type *type-value*	(OPTIONAL) Enter the keywords `metric-type` then one of the following: • 1 = for OSPF External type 1 • 2 = for OSPF External type 2
route-map *map-name*	(OPTIONAL) Enter the keywords `route-map` then the name of the route map.
tag *tag-value*	(OPTIONAL) Enter the keyword `tag` to set the tag for routes redistributed into OSPF. The range is from 0 to 4294967295.

Defaults	Not configured.
Command Modes	ROUTER OSPF
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

router-id

To configure a fixed router ID, use this command.

Syntax	`router-id ip-address` To remove the fixed router ID, use the `no router-id ip-address` command.
Parameters	*ip-address* — Enter the router ID in the IP address format.
Defaults	none.
Command Modes	ROUTER OSPF
Command History	**Version 8.3.16.1** — Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	You can configure an arbitrary value in the IP address format for each router. However, each router ID must be unique. If you use this command on an OSPF router process, which is already active (that is, has neighbors), a prompt reminding you that changing the router-id brings down the existing OSPF adjacency. The new router ID is effective at the next reload.

Example

```
Dell(conf)#router ospf 100
Dell(conf-router_ospf)#router-id 1.1.1.1
Changing router-id will bring down existing OSPF adjacency [y/
n]:

Dell(conf-router_ospf)#show config
!
router ospf 100
router-id 1.1.1.1
Dell(conf-router_ospf)#no router-id
Changing router-id will bring down existing OSPF adjacency [y/
n]:
Dell#
```

router ospf

To configure an OSPF instance, enter ROUTER OSPF mode.

Syntax	`router ospf process-id` To clear an OSPF instance, use the `no router ospf process-id` command.
Parameters	*process-id* — Enter a number for the OSPF instance. The range is from 1 to 65535.
Defaults	Not configured.

Command Modes	CONFIGURATION
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	You must have an IP address assigned to an interface to enter ROUTER OSPF mode and configure OSPF.

Example

```
Dell(conf)#router ospf 2
Dell(conf-router_ospf)#
```

show config

Display the non-default values in the current OSPF configuration.

Syntax	`show config`
Command Modes	ROUTER OSPF
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell(conf-router_ospf)#show config
!
router ospf 3
passive-interface FastEthernet 0/1
Dell(conf-router_ospf)#
```

show ip ospf

Display information on the OSPF process configured on the switch.

Syntax

`show ip ospf process-id`

Parameters

process-id	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information	If you delete all the network area commands for Area 0, the `show ip ospf` command output does not list Area 0. The following describes the `show ip ospf` command shown in the following example.

Line Beginning with	Description
"Routing Process..."	Displays the OSPF process ID and the IP address associated with the process ID.
"Supports only..."	Displays the number of Type of Service (TOS) rouse supported.
"SPF schedule..."	Displays the delay and hold time configured for this process ID.
"Convergence Level"	
"Min LSA...."	Displays the intervals set for LSA transmission and acceptance.
"Number of..."	Displays the number and type of areas configured for this process ID.

Example

```
Dell#show ip ospf 10
Routing Process ospf 10 with ID 1.1.1.1 Virtual router default-
vrf
Supports only single TOS (TOS0) routes
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Convergence Level 0
Min LSA origination 0 msec, Min LSA arrival 1000 msec
Min LSA hold time 5000 msec, Max LSA wait time 5000 msec
Number of area in this router is 1, normal 1 stub 0 nssa 0
    Area BACKBONE (0)
      Number of interface in this area is 1
      SPF algorithm executed 205 times
      Area ranges are
Dell#
```

Related Commands

show ip ospf database — displays information about the OSPF routes configured.

show ip ospf interface — displays the OSPF interfaces configured.

show ip ospf neighbor — displays the OSPF neighbors configured.

show ip ospf asbr

Display all autonomous system boundary router (ASBR) routers visible to OSPF.

Syntax `show ip ospf process-id asbr`

Parameters	*process-id*	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To isolate problems with external routes, use this command. In OSPF, external routes are calculated by adding the LSA cost to the cost of reaching the ASBR router. If an external route does not have the correct cost, use this command to determine if the path to the originating router is correct. The display output is not sorted in any order.

NOTE: ASBRs that are not in directly connected areas are also displayed.

You can determine if an ASBR is in a directly connected area (or not) by the flags. For ASBRs in a directly connected area, E flags are set. In the following example, router 1.1.1.1 is in a directly connected area since the Flag is E/-/-/. For remote ASBRs, the E flag is clear (-/-/-/).

Example

```
Dell#show ip ospf 1asbr

RouterID  Flags   Cost Nexthop   Interface Area
3.3.3.3   -/-/-/  2   10.0.0.2   Gi 0/1    1
1.1.1.1   E/-/-/  0   0.0.0.0    -         0
Dell#
```

show ip ospf database

Display all LSA information. If you do not enable OSPF on the switch, no output is generated.

Syntax `show ip ospf process-id database [database-summary]`

Parameters	*process-id*	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
	database-summary	(OPTIONAL) Enter the keywords `database-summary` to the display the number of LSA types in each area and the total number of LSAs.

Command Modes	- EXEC - EXEC Privilege
Command History	Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show ip ospf` *`process-id`* `database` command shown in the following example.

Field	Description
Link ID	Identifies the router ID.
ADV Router	Identifies the advertising router's ID.
Age	Displays the link state age.
Seq#	Identifies the link state sequence number. This number allows you to identify old or duplicate link state advertisements.
Checksum	Displays the Fletcher checksum of an LSA's complete contents.
Link count	Displays the number of interfaces for that router.

Example

```
Dell>show ip ospf 1 database

     OSPF Router with ID (11.1.2.1) (Process ID 1)
                Router (Area 0.0.0.0)
Link ID      ADV Router   Age  Seq#       Checksum Link count
11.1.2.1     11.1.2.1     673  0x80000005 0x707e   2
13.1.1.1     13.1.1.1     676  0x80000097 0x1035   2
192.68.135.2 192.68.135.2 1419 0x80000294 0x9cbd   1

               Network (Area 0.0.0.0)
Link ID      ADV Router   Age  Seq#       Checksum
10.2.3.2     13.1.1.1     676  0x80000003 0x6592
10.2.4.2     192.68.135.2 908  0x80000055 0x683e

               Type-5 AS External
Link ID      ADV Router   Age  Seq#       Checksum Tag
0.0.0.0      192.68.135.2 908  0x80000052 0xeb83   100
1.1.1.1      192.68.135.2 908  0x8000002a 0xbd27   0
10.1.1.0     11.1.2.1     718  0x80000002 0x9012   0
10.1.2.0     11.1.2.1     718  0x80000002 0x851c   0
10.2.2.0     11.1.2.1     718  0x80000002 0x7927   0
10.2.3.0     11.1.2.1     718  0x80000002 0x6e31   0
10.2.4.0     13.1.1.1     1184 0x80000068 0x45db   0
11.1.1.0     11.1.2.1     718  0x80000002 0x831e   0
11.1.2.0     11.1.2.1     718  0x80000002 0x7828   0
12.1.2.0     192.68.135.2 1663 0x80000054 0xd8d6   0
13.1.1.0     13.1.1.1     1192 0x8000006b 0x2718   0
13.1.2.0     13.1.1.1     1184 0x8000006b 0x1c22   0
172.16.1.0   13.1.1.1     148  0x8000006d 0x533b   0
Dell>
```

Related Commands	show ip ospf database asbr-summary — displays only ASBR summary LSA information.

show ip ospf database asbr-summary

Display information about autonomous system (AS) boundary LSAs.

Syntax

```
show ip ospf process-id database asbr-summary [link-state-id]
[adv-router ip-address]
```

Parameters

process-id	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
link-state-id	(OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following: • the network's IP address for Type 3 LSAs or Type 5 LSAs • the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs • the default destination (0.0.0.0) for Type 5 LSAs
adv-router *ip-address*	(OPTIONAL) Enter the keywords `adv-router` and the ip-address to display only the LSA information about that router.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show ip ospf database asbr-summary` command shown in the following example.

Field	Description
LS Age	Displays the LSA's age.
Options	Displays the optional capabilities available on router. The following options can be found in this item: • TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service. • DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits.

Field	Description
	- E or No E is displayed on whether the originating router can accept AS External LSAs.
LS Type	Displays the LSA's type.
Link State ID	Displays the Link State ID.
Advertising Router	Identifies the advertising router's ID.
Checksum	Displays the Fletcher checksum of the LSA's complete contents.
Length	Displays the length in bytes of the LSA.
Network Mask	Displays the network mask implemented on the area.
TOS	Displays the Type of Service (TOS) options. Option 0 is the only option.
Metric	Displays the LSA metric.

Example

```
Dell#show ip ospf 100 database asbr-summary

     OSPF Router with ID (1.1.1.10) (Process ID 100)

       Summary Asbr (Area 0.0.0.0)

LS age: 1437
Options: (No TOS-capability, No DC, E)
LS type: Summary Asbr
Link State ID: 103.1.50.1
Advertising Router: 1.1.1.10
LS Seq Number: 0x8000000f
Checksum: 0x8221
Length: 28
Network Mask: /0
      TOS: 0 Metric: 2

LS age: 473
Options: (No TOS-capability, No DC, E)
LS type: Summary Asbr
Link State ID: 104.1.50.1
Advertising Router: 1.1.1.10
LS Seq Number: 0x80000010
Checksum: 0x4198
Length: 28
--More--
```

Related Commands

show ip ospf database — displays OSPF database information.

show ip ospf database external

Display information on the AS external (type 5) LSAs.

Syntax

```
show ip ospf process-id database external [link-state-id] [adv-router ip-address]
```

Parameters

process-id	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
link-state-id	(OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following: • the network's IP address for Type 3 LSAs or Type 5 LSAs • the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs • the default destination (0.0.0.0) for Type 5 LSAs
adv-router *ip-address*	(OPTIONAL) Enter the keywords `adv-router` and the ip-address to display only the LSA information about that router.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show ip ospf process-id database external` command shown in the following example.

Field	Description
LS Age	Displays the LSA's age.
Options	Displays the optional capabilities available on router. The following options can be found in this item: • TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service. • DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits. • E or No E is displayed on whether the originating router can accept AS External LSAs.
LS Type	Displays the LSA's type.
Link State ID	Displays the Link State ID.

Field	Description
Advertising Router	Identifies the router ID of the LSA's originating router.
LS Seq Number	Identifies the link state sequence number. This number enables you to identify old or duplicate LSAs.
Checksum	Displays the Fletcher checksum of the LSA's complete contents.
Length	Displays the length in bytes of the LSA.
Network Mask	Displays the network mask implemented on the area.
Metrics Type	Displays the external type.
TOS	Displays the Type of Service (TOS) options. Option 0 is the only option.
Metric	Displays the LSA metric.
Forward Address	Identifies the address of the forwarding router. Data traffic is forwarded to this router. If the forwarding address is 0.0.0.0, data traffic is forwarded to the originating router.
External Route Tag	Displays the 32-bit field attached to each external route. The OSPF protocol does not use this field, but you can use the field for external route management.

Example

```
Dell#show ip ospf 1 database external

    OSPF Router with ID (20.20.20.5) (Process ID 1)

         Type-5 AS External

LS age: 612
Options: (No TOS-capability, No DC, E)
LS type: Type-5 AS External
Link State ID: 12.12.12.2
Advertising Router: 20.31.3.1
LS Seq Number: 0x80000007
Checksum: 0x4cde
Length: 36
Network Mask: /32
     Metrics Type: 2
     TOS: 0
     Metrics: 25
     Forward Address: 0.0.0.0
     External Route Tag: 43

LS age: 1868
Options: (No TOS-capability, DC)
LS type: Type-5 AS External
Link State ID: 24.216.12.0
Advertising Router: 20.20.20.8
LS Seq Number: 0x80000005
Checksum: 0xa00e
Length: 36
Network Mask: /24
     Metrics Type: 2
     TOS: 0
     Metrics: 1
     Forward Address: 0.0.0.0
     External Route Tag: 701
Dell#
```

Related Commands	show ip ospf database — displays OSPF database information.

show ip ospf database network

Display the network (type 2) LSA information.

Syntax

`show ip ospf process-id database network [link-state-id] [adv-router ip-address]`

Parameters

process-id	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
link-state-id	(OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following: • the network's IP address for Type 3 LSAs or Type 5 LSAs • the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs • the default destination (0.0.0.0) for Type 5 LSAs
adv-router *ip-address*	(OPTIONAL) Enter the keywords `adv-router` and the ip-address to display only the LSA information about that router.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show ip ospf process-id database network` command shown in the following example.

Field	Description
LS Age	Displays the LSA's age.
Options	Displays the optional capabilities available on router. The following options can be found in this item: • TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service.

Field	Description
	• DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits. • E or No E is displayed on whether the originating router can accept AS External LSAs.
LS Type	Displays the LSA's type.
Link State ID	Displays the Link State ID.
Advertising Router	Identifies the router ID of the LSA's originating router.
Checksum	Identifies the link state sequence number. This number enables you to identify old or duplicate LSAs.
Length	Displays the Fletcher checksum of an LSA's complete contents.
Network Mask	Displays the length in bytes of the LSA.
Attached Router	Identifies the IP address of routers attached to the network.

Example

```
Dell#show ip ospf 1 data network

    OSPF Router with ID (20.20.20.5) (Process ID 1)

        Network (Area 0.0.0.0)
 LS age: 1372
Options: (No TOS-capability, DC, E)
LS type: Network
Link State ID: 202.10.10.2
Advertising Router: 20.20.20.8
LS Seq Number: 0x80000006
Checksum: 0xa35
Length: 36
Network Mask: /24
     Attached Router: 20.20.20.8
     Attached Router: 20.20.20.9
     Attached Router: 20.20.20.7

         Network (Area 0.0.0.1)

LS age: 252
Options: (TOS-capability, No DC, E)
LS type: Network
Link State ID: 192.10.10.2
Advertising Router: 192.10.10.2
LS Seq Number: 0x80000007
Checksum: 0x4309
Length: 36
Network Mask: /24
     Attached Router: 192.10.10.2
     Attached Router: 20.20.20.1
     Attached Router: 20.20.20.5
Dell#
```

Related Commands

show ip ospf database — displays OSPF database information.

show ip ospf database nssa-external

Display NSSA-External (type 7) LSA information.

Syntax

```
show ip ospf database nssa-external [link-state-id] [adv-router
ip-address]
```

Parameters

link-state-id	(OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following: • the network's IP address for Type 3 LSAs or Type 5 LSAs • the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs • the default destination (0.0.0.0) for Type 5 LSAs
adv-router *ip-address*	(OPTIONAL) Enter the keywords `adv-router` and the ip-address to display only the LSA information about that router.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

show ip ospf database — displays OSPF database information.

show ip ospf database opaque-area

Display the opaque-area (type 10) LSA information.

Syntax

```
show ip ospf process-id database opaque-area [link-state-id]
[adv-router ip-address]
```

Parameters

process-id	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
link-state-id	(OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following: • the network's IP address for Type 3 LSAs or Type 5 LSAs • the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs • the default destination (0.0.0.0) for Type 5 LSAs

adv-router *ip-address*	(OPTIONAL) Enter the keywords `adv-router` and the ip-address to display only the LSA information about that router.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show ip ospf` *`process-id`* `database opaque-area` command shown in the following example.

Item	Description
LS Age	Displays the LSA's age.
Options	Displays the optional capabilities available on router. The following options can be found in this item: • TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service. • DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits. • E or No E is displayed on whether the originating router can accept AS External LSAs.
LS Type	Displays the LSA's type.
Link State ID	Displays the Link State ID.
Advertising Router	Identifies the advertising router's ID.
Checksum	Displays the Fletcher checksum of the LSA's complete contents.
Length	Displays the length in bytes of the LSA.
Opaque Type	Displays the Opaque type field (the first 8 bits of the Link State ID).
Opaque ID	Displays the Opaque type-specific ID (the remaining 24 bits of the Link State ID).

Example

```
Dell>show ip ospf 1 database opaque-area

    OSPF Router with ID (3.3.3.3) (Process ID 1)
         Type-10 Opaque Link Area (Area 0)

LS age: 1133
Options: (No TOS-capability, No DC, E)
LS type: Type-10 Opaque Link Area
Link State ID: 1.0.0.1
Advertising Router: 10.16.1.160
LS Seq Number: 0x80000416
```

```
Checksum: 0x376
Length: 28
Opaque Type: 1
Opaque ID: 1
Unable to display opaque data

LS age: 833
Options: (No TOS-capability, No DC, E)
LS type: Type-10 Opaque Link Area
Link State ID: 1.0.0.2
Advertising Router: 10.16.1.160
LS Seq Number: 0x80000002
Checksum: 0x19c2
--More--
```

Related Commands

show ip ospf database — displays OSPF database information.

show ip ospf database opaque-as

Display the opaque-as (type 11) LSA information.

Syntax

`show ip ospf process-id database opaque-as [link-state-id] [adv-router ip-address]`

Parameters

process-id	Enter the OSPF process ID to show a specific process. If you do not enter the process ID, the command applies only to the first OSPF process.
link-state-id	(OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following: • the network's IP address for Type 3 LSAs or Type 5 LSAs • the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs • the default destination (0.0.0.0) for Type 5 LSAs
adv-router *ip-address*	(OPTIONAL) Enter the keywords `adv-router` and the ip-address to display only the LSA information about that router.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

show ip ospf database — displays OSPF database information.

show ip ospf database opaque-link

Display the opaque-link (type 9) LSA information.

Syntax	`show ip ospf` *`process-id`* `database opaque-link [`*`link-state-id`*`] [adv-router` *`ip-address`*`]`

Parameters

process-id	Enter the OSPF process ID to show a specific process. If you do not enter the process ID, the command applies only to the first OSPF process.
link-state-id	(OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following: • the network's IP address for Type 3 LSAs or Type 5 LSAs • the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs • the default destination (0.0.0.0) for Type 5 LSAs
adv-router *ip-address*	(OPTIONAL) Enter the keywords `adv-router` then the IP address of an Advertising Router to display only the LSA information about that router.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

show ip ospf database — displays OSPF database information.

show ip ospf database router

Display the router (type 1) LSA information.

Syntax	`show ip ospf` *`process-id`* `database router [`*`link-state-id`*`] [adv-router` *`ip-address`*`]`

Parameters

process-id	Enter the OSPF Process ID to show a specific process. If you do not enter a process ID, the command applies only to the first OSPF process.
link-state-id	(OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following:

	- the network's IP address for Type 3 LSAs or Type 5 LSAs - the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs - the default destination (0.0.0.0) for Type 5 LSAs
adv-router *ip-address*	(OPTIONAL) Enter the keywords `adv-router` then the IP address of an Advertising Router to display only the LSA information about that router.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show ip ospf process-id database router` command shown in the following example.

Item	Description
LS Age	Displays the LSA age.
Options	Displays the optional capabilities available on router. The following options can be found in this item: - TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service. - DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits. - E or No E is displayed on whether the originating router can accept AS External LSAs.
LS Type	Displays the LSA type.
Link State ID	Displays the Link State ID.
Advertising Router	Identifies the router ID of the LSA's originating router.
LS Seq Number	Displays the link state sequence number. This number detects duplicate or old LSAs.
Checksum	Displays the Fletcher checksum of an LSA's complete contents.
Length	Displays the length in bytes of the LSA.
Number of Links	Displays the number of active links to the type of router (Area Border Router or AS Boundary Router) listed in the previous line.
Link connected to:	Identifies the type of network to which the router is connected.

Item	Description
(Link ID)	Identifies the link type and address.
(Link Data)	Identifies the router interface address.
Number of TOS Metric	Lists the number of TOS metrics.
TOS 0 Metric	Lists the number of TOS 0 metrics.

Example

```
Dell#show ip ospf 100 database router

     OSPF Router with ID (1.1.1.10) (Process ID 100)

         Router (Area 0)

LS age: 967
Options: (No TOS-capability, No DC, E)
LS type: Router
Link State ID: 1.1.1.10
Advertising Router: 1.1.1.10
LS Seq Number: 0x8000012f
Checksum: 0x3357
Length: 144
AS Boundary Router
Area Border Router
  Number of Links: 10

  Link connected to: a Transit Network
    (Link ID) Designated Router address: 192.68.129.1
    (Link Data) Router Interface address: 192.68.129.1
    Number of TOS metric: 0
       TOS 0 Metric: 1

  Link connected to: a Transit Network
    (Link ID) Designated Router address: 192.68.130.1
    (Link Data) Router Interface address: 192.68.130.1
    Number of TOS metric: 0
       TOS 0 Metric: 1

  Link connected to: a Transit Network
    (Link ID) Designated Router address: 192.68.142.2
    (Link Data) Router Interface address: 192.68.142.2
    Number of TOS metric: 0
       TOS 0 Metric: 1

  Link connected to: a Transit Network
    (Link ID) Designated Router address: 192.68.141.2
    (Link Data) Router Interface address: 192.68.141.2
    Number of TOS metric: 0
       TOS 0 Metric: 1

  Link connected to: a Transit Network
    (Link ID) Designated Router address: 192.68.140.2
    (Link Data) Router Interface address: 192.68.140.2
    Number of TOS metric: 0
       TOS 0 Metric: 1

Link connected to: a Stub Network
    (Link ID) Network/subnet number: 11.1.5.0
--More--
```

Related Commands	[show ip ospf database](#) — displays OSPF database information.

show ip ospf database summary

Display the network summary (type 3) LSA routing information.

Syntax

```
show ip ospf process-id database summary [link-state-id] [adv-
router ip-address]
```

Parameters

process-id	Enter the OSPF process ID to show a specific process. If you do not enter a process ID, the command applies only to the first OSPF process.
link-state-id	(OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following: • the network's IP address for Type 3 LSAs or Type 5 LSAs • the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs • the default destination (0.0.0.0) for Type 5 LSAs
adv-router *ip-address*	(OPTIONAL) Enter the keywords `adv-router` then the IP address of an Advertising Router to display only the LSA information about that router.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show ip ospf process-id database summary` command shown in the following example.

Item	Description
LS Age	Displays the LSA age.
Options	Displays the optional capabilities available on router. The following options can be found in this item: • TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service. • DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits.

Item	Description
	• E or No E is displayed on whether the originating router can accept AS External LSAs.
LS Type	Displays the LSA type.
Link State ID	Displays the Link State ID.
Advertising Router	Identifies the router ID of the LSA’s originating router.
LS Seq Number	Displays the link state sequence number. This number allows you to identify old or duplicate LSAs.
Checksum	Displays the Fletcher checksum of an LSA’s complete contents.
Length	Displays the length in bytes of the LSA.
Network Mask	Displays the network mask implemented on the area.
TOS	Displays the TOS options. Option 0 is the only option.
Metric	Displays the LSA metrics.

Example

```
#show ip ospf 100 database summary

    OSPF Router with ID (1.1.1.10) (Process ID 100)

        Summary Network (Area 0.0.0.0)

LS age: 1551
Options: (No TOS-capability, DC, E)
LS type: Summary Network
Link State ID: 192.68.16.0
Advertising Router: 192.168.17.1
LS Seq Number: 0x80000054
Checksum: 0xb5a2
Length: 28
Network Mask: /24
    TOS: 0 Metric: 1

LS age: 9
Options: (No TOS-capability, No DC, E)
LS type: Summary Network
Link State ID: 192.68.32.0
Advertising Router: 1.1.1.10
LS Seq Number: 0x80000016
Checksum: 0x987c
Length: 28
Network Mask: /24
   TOS: 0 Metric: 1

LS age: 7
Options: (No TOS-capability, No DC, E)
LS type: Summary Network
Link State ID: 192.68.33.0
Advertising Router: 1.1.1.10
LS Seq Number: 0x80000016
Checksum: 0x1241
Length: 28
Network Mask: /26
   TOS: 0 Metric: 1
```

```
#
```

Related Commands

[show ip ospf database](#) — displays OSPF database information.

show ip ospf interface

Display the OSPF interfaces configured. If OSPF is not enabled on the switch, no output is generated.

Syntax `show ip ospf process-id interface [interface]`

Parameters

process-id	Enter the OSPF process ID to show a specific process. If you do not enter a process ID, the command applies only to the first OSPF process.
interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For the null interface, enter the keyword `null` then zero (0). • For Loopback interfaces, enter the keyword `loopback` then a number from 0 to 16383. • For Port Channel groups, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a VLAN, enter the keyword `vlan` then the VLAN ID. The range is from 1 to 4094. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show ip ospf process-id interface` command shown in the following example.

Item	Description
GigabitEthernet...	This line identifies the interface type slot/port and the status of the OSPF protocol on that interface.
Internet Address...	This line displays the IP address, network mask and area assigned to this interface.

Item	Description
Process ID...	This line displays the OSPF Process ID, Router ID, Network type and cost metric for this interface.
Transmit Delay...	This line displays the interface's settings for Transmit Delay, State, and Priority. In the State setting, BDR is Backup Designated Router.
Designated Router...	This line displays the ID of the Designated Router and its interface address.
Backup Designated...	This line displays the ID of the Backup Designated Router and its interface address.
Timer intervals...	This line displays the interface's timer settings for Hello interval, Dead interval, Transmit Delay (Wait), and Retransmit Interval.
Hello due...	This line displays the amount time until the next Hello packet is sent out this interface.
Neighbor Count...	This line displays the number of neighbors and adjacent neighbors. Listed below this line are the details about each adjacent neighbor.

Example

```
Dell>show ip ospf int

TenGigabitEthernet 13/17 is up, line protocol is up
  Internet Address 192.168.1.2/30, Area 0.0.0.1
  Process ID 1, Router ID 192.168.253.2, Network Type
BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.253.2, Interface address
192.168.1.2
  Backup Designated Router (ID) 192.168.253.1, Interface
address 192.168.1.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
    Hello due in 00:00:02
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.253.1 (Backup Designated
Router)

TenGigabitEthernet 13/23 is up, line protocol is up
  Internet Address 192.168.0.1/24, Area 0.0.0.1
  Process ID 1, Router ID 192.168.253.2, Network Type
BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DROTHER, Priority 1
  Designated Router (ID) 192.168.253.5, Interface address
192.168.0.4
  Backup Designated Router (ID) 192.168.253.3, Interface
address 192.168.0.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
    Hello due in 00:00:08
  Neighbor Count is 3, Adjacent neighbor count is 2
    Adjacent with neighbor 192.168.253.5 (Designated Router)
    Adjacent with neighbor 192.168.253.3 (Backup Designated
Router)
```

```
Loopback 0 is up, line protocol is up
  Internet Address 192.168.253.2/32, Area 0.0.0.1
  Process ID 1, Router ID 192.168.253.2, Network Type
LOOPBACK, Cost: 1
Loopback interface is treated as a stub Host.
Dell>
```

show ip ospf neighbor

Display the OSPF neighbors connected to the local router.

Syntax `show ip ospf process-id neighbor`

Parameters

process-id	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.

Command Modes EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information The following describes the `show ip ospf process-id neighbor` command shown in the following example.

Item	Description
Neighbor ID	Displays the neighbor router ID.
Pri	Displays the priority assigned neighbor.
State	Displays the OSPF state of the neighbor.
Dead Time	Displays the expected time until the system declares the neighbor dead.
Address	Displays the IP address of the neighbor.
Interface	Displays the interface type slot/port information.
Area	Displays the neighbor's area (process ID).

Example

```
Dell#show ip ospf 34 neighbor

Neighbor ID Pri State       Dead Time Address  Interface Area
20.20.20.7  1 FULL/DR     00:00:32 182.10.10.3 Gi 0/0 0.0.0.2
192.10.10.2 1 FULL/DR     00:00:37 192.10.10.2 Gi 0/1 0.0.0.1
20.20.20.1  1 FULL/DROTHER00:00:36 192.10.10.4 Gi 0/1 0.0.0.1
Dell#
```

show ip ospf routes

Display routes OSPF calculates and stores in OSPF RIB.

Syntax `show ip ospf process-id routes`

Parameters

process-id	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

This command is useful in isolating routing problems between the OSPF and the RTM. For example, if a route is missing from the RTM/FIB but is visible from the display output of this command, the problem is with downloading the route to the RTM.

This command has the following limitations:

- The display output is sorted by prefixes; intra-area ECMP routes are not displayed together.
- For Type 2 external routes, Type 1 cost is not displayed.

Example

```
Dell#show ip ospf 100 route

Prefix        Cost Nexthop   Interface Area  Type
1.1.1.1        1   0.0.0.0   Lo 0      0     Intra-Area
3.3.3.3        2   13.0.0.3  Gi 0/47   1     Intra-Area
13.0.0.0       1   0.0.0.0   Gi 0/47   0     Intra-Area
150.150.150.0  2   13.0.0.3  Gi 0/47   -     External
172.30.1.0     2   13.0.0.3  Gi 0/47   1     Intra-Area
Dell#
```

show ip ospf statistics

Display OSPF statistics.

Syntax `show ip ospf process-id statistics global | [interface name {neighbor router-id}]`

Parameters

process-id	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.

global	Enter the keyword `global` to display the packet counts received on all running OSPF interfaces and packet counts OSPF neighbors receive and transmit.
interface ***name***	(OPTIONAL) Enter the keyword `interface` then one of the following interface keywords and slot/port or number information: • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For Port Channel groups, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.
neighbor ***router-id***	(OPTIONAL) Enter the keyword `neighbor` then the neighbor's router-id in dotted decimal format (A.B.C.D.).

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show ip ospf statistics` *`process-id`* `global` command shown in the following example.

Row Heading	Description
Total	Displays the total number of packets the OSPF process receives/transmits.
Error	Displays the error count while receiving and transmitting packets by the OSPF process.
Hello	Number of OSPF Hello packets.
DDiscr	Number of database description packets.
LSReq	Number of link state request packets.
LSUpd	Number of link state update packets.
LSAck	Number of link state acknowledgement packets.
TxQ-Len	The transmission queue length.
RxQ-Len	The reception queue length.
Tx-Mark	The highest number mark in the transmission queue.
Rx-Mark	The highest number mark in the reception queue.

Row Heading	Description
Hello-Q	The queue, for transmission or reception, for the hello packets.
LSR-Q	The queue, for transmission or reception, for the link state request packets.
Other-Q	The queue, for transmission or reception, for the link state acknowledgement, database description, and update packets.

The following describes the error definitions for the `show ip ospf statistics` *`process-id`* `global` command.

Error Type	Description
Intf_Down	Received packets on an interface that is either down or OSPF is not enabled.
Non-Dr	Received packets with a destination address of ALL_DRS even though SELF is not a designated router.
Self-Org	Receive the self originated packet.
Wrong_Len	The received packet length is different to what was indicated in the OSPF header.
Invld-Nbr	LSA, LSR, LSU, and DDB are received from a peer which is not a neighbor peer.
Nbr-State	LSA, LSR, and LSU are received from a neighbor with stats less than the loading state.
Auth-Error	Simple authentication error.
MD5-Error	MD5 error
Cksum-Err	Checksum Error
Version	Version mismatch
AreaMismatch	Area mismatch
Conf-Issue	The received hello packet has a different hello or dead interval than the configuration.
No-Buffer	Buffer allocation failure.
Seq-no	A sequence no errors occurred during the database exchange process.
Socket	Socket Read/Write operation error.
Q-overflow	Packets dropped due to queue overflow.
Unknown-Pkt	Received packet is not an OSPF packet.

Example

```
Dell#show ip ospf 10 statistics global

  OSPF Packet Count
```

```
       Total Error Hello DDiscr LSReq LSUpd
LSAck
RX        34     0    26      2     1    3
2
TX        34     0    25      3     1    3
2

  OSPF Global Queue Length
         TxQ-Len RxQ-Len Tx-Mark Rx-Mark
Hello-Q        0      0       1        1
LSR-Q          0      0       1        1
Other-Q        0      0       2        2

  Error packets (Receive statistics)
Intf-Down   0   Non-Dr      0   Self-Org 0
Wrong-Len   0   Invld-Nbr   0   Nbr-State
0
Auth-Err    0   MD5-Err     0   Chksum 0
Version     0   AreaMis     0   Conf-Issues
0
No-Buffer   0   Seq-No      0  Socket 0
Q-OverFlow  0   Unknown-Pkt 0  RtidZero
0
Error packets (Transmit statistics)
Socket Errors 0
Dell#
```

Usage Information

The `show ip ospf` *`process-id`* `statistics` command displays the error packet count received on each interface as:

- The hello-timer remaining value for each interface
- The wait-timer remaining value for each interface
- The grace-timer remaining value for each interface
- The packet count received and transmitted for each neighbor
- Dead timer remaining value for each neighbor
- Transmit timer remaining value for each neighbor
- The LSU Q length and its highest mark for each neighbor
- The LSR Q length and its highest mark for each neighbor

Example (Statistics)

```
Dell#show ip ospf 10 statistics
Interface TenGigabitEthernet 4/45
  Error packets (Receive statistics)
    Intf-Down    0 Non-Dr        0 Self-Org    0
    Wrong-Len    0 Invld-Nbr     0 Nbr-State   0
    Auth-Error   0 MD5-Error     0 Cksum-Err   0
    Version      0 AreaMisMatch  0 Conf-Issue  0
    SeqNo-Err    0 Unknown-Pkt   0 Bad-LsReq   0
    RtidZero     0
  Neighbor ID 3.1.1.2
    Packet Statistics
           Hello DDiscr LSReq LSUpd LSAck
      RX      47      2     1     3     2
      TX      46      3     1     3     2
    Timers
      Hello     1  Wait         0      Grace 0
      Dead     37  Transmit     0
    Queue Statistics
      LSU-Q-Len   0   LSU-Q-Wmark   1
      LSR-Q-Len    0    LSR-Q-Wmark    1
Dell#
```

Related Commands clear ip ospf statistics — clears the packet statistics in all interfaces and neighbors.

show ip ospf timers rate-limit

Show the LSA currently in the queue waiting for timers to expire.

Syntax `show ip ospf process-id timers rate-limit`

Parameters

process-id	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show ip ospf 10 timers rate-limit

List of LSAs in rate limit Queue
LSA id: 1.1.1.0 Type: 3 Adv Rtid: 3.3.3.3 Expiry time:
00:00:09.111
LSA id: 3.3.3.3 Type: 1 Adv Rtid: 3.3.3.3 Expiry time:
00:00:23.96
Dell#
```

show ip ospf topology

Display routers in directly connected areas.

Syntax `show ip ospf process-id topology`

Parameters

process-id	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.

Defaults none

Command Modes	- EXEC - EXEC Privilege
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	To isolate problems with inter-area and external routes, use this command. In OSPF inter-area and external routes are calculated by adding LSA cost to the cost of reaching the router. If an inter-area or external route is not of correct cost, the display can determine if the path to the originating router is correct or not.

Example

```
Dell#show ip ospf 1 topology

Router ID  Flags Cost  Nexthop   Interface Area
3.3.3.3    E/B/-/ 1    20.0.0.3  Gi 13/1   0
1.1.1.1    E/-/-/ 1    10.0.0.1  Gi 7/1    1
Dell#
```

summary-address

To advertise one external route, set the OSPF ASBR.

Syntax

`summary-address ip-address mask [not-advertise] [tag tag-value]`

To disable summary address, use the `no summary-address ip-address mask` command.

Parameters

ip-address	Specify the IP address in dotted decimal format of the address to summarize.
mask	Specify the mask in dotted decimal format of the address to summarize.
not-advertise	(OPTIONAL) Enter the keywords `not-advertise` to suppress that match the network prefix/mask pair.
tag *tag-value*	(OPTIONAL) Enter the keyword `tag` then a value to match on routes redistributed through a route map. The range is from 0 to 4294967295.

Defaults	Not configured.
Command Modes	ROUTER OSPF
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The `area range` command summarizes routes for the different areas.

With the `not-advertise` parameter configured, you can use this command to filter out some external routes. For example, if you want to redistribute static routes to OSPF, but you don't want OSPF to advertise routes with prefix 1.1.0.0, you can configure the summary-address 1.1.0.0 255.255.0.0 not-advertise to filter out all the routes fall in range 1.1.0.0/16.

Related Commands	area range — summarizes routes within an area.

timers spf

Set the time interval between when the switch receives a topology change and starts a shortest path first (SPF) calculation.

Syntax

```
timers spf delay holdtime
```

To return to the default, use the `no timers spf` command.

Parameters

delay	Enter a number as the delay. The range is from 0 to 4294967295. The default is **5 seconds**.
holdtime	Enter a number as the hold time. The range is from 0 to 4294967295. The default is **10 seconds**.

Defaults

- delay = 5 seconds
- holdtime = 10 seconds

Command Modes: ROUTER OSPF

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information: Setting the *delay* and *holdtime* parameters to a low number enables the switch to an alternate path quickly but requires more CPU usage.

timers throttle lsa all

Configure LSA transmit intervals.

Syntax

```
timers throttle lsa all {start-interval | hold-interval | max-interval}
```

To return to the default, use the `no timers throttle lsa` command.

Parameters

start-interval	Set the minimum interval between initial sending and resending the same LSA. The range is from 0 to 600,000 milliseconds.

hold-interval	Set the next interval to send the same LSA. This interval is the time between sending the same LSA after the start-interval has been attempted. The range is from 1 to 600,000 milliseconds.
max-interval	Set the maximum amount of time the system waits before sending the LSA. The range is from 1 to 600,000 milliseconds.

Defaults

- start-interval: **0 msec**
- hold-interval: **5000 msec**
- max-interval: **5000 msec**

Command Modes

ROUTER OSPF

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

LSAs are sent after the start-interval and then after hold-interval until the maximum interval is reached. In throttling, exponential backoff is used when sending same LSA, so that the interval is multiplied until the maximum time is reached. For example, if the *start-interval 5000* and *hold-interval 1000* and *max-interval 100,000*, the LSA is sent at 5000 msec, then 1000 msec, then 2000 msec, them 4000 until 100,000 msec is reached.

timers throttle lsa arrival

Configure the LSA acceptance intervals.

Syntax

`timers throttle lsa arrival` *`arrival-time`*

To return to the default, use the `no timers throttle lsa` command.

Parameters

arrival-time	Set the interval between receiving the same LSA repeatedly, to allow sufficient time for the system to accept the LSA. The range is from 0 to 600,000 milliseconds.

Defaults

1000 msec

Command Modes

ROUTER OSPF

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

OSPFv3 Commands

Open shortest path first version 3 (OSPFv3) for IPv6 is supported on the MXL Switch platform.

The fundamental mechanisms of OSPF (flooding, DR election, area support, SPF calculations, and so on) remain unchanged. However, OSPFv3 runs on a per-link basis instead of on a per-IP-subnet basis. Most changes were necessary to handle the increased address size of IPv6.

The Dell Networking implementation of OSPFv3 is based on IETF RFC 2740.

area authentication

Configure an IPsec authentication policy for OSPFv3 packets in an OFSPFv3 area.

Syntax

```
area area-id authentication ipsec spi number {MD5 | SHA1} [key-encryption-type] key
```

Parameters

area *area-id*	Area for which OSPFv3 traffic is to be authenticated. For area-id, you can enter a number. The range is from 0 to 4294967295.
ipsec spi *number*	Security Policy index (SPI) value that identifies an IPsec security policy. The range is from 256 to 4294967295.
MD5 | SHA1	Authentication type: Message Digest 5 (MD5) or Secure Hash Algorithm 1 (SHA-1).
key-encryption-type	(OPTIONAL) Specifies if the key is encrypted. The values are 0 (key is not encrypted) or 7 (key is encrypted).
key	Text string used in authentication. For MD5 authentication, the key must be 32 hex digits (non-encrypted) or 64 hex digits (encrypted). For SHA-1 authentication, the key must be 40 hex digits (non-encrypted) or 80 hex digits (encrypted).

Defaults Not configured.

Command Modes ROUTER OSPFv3

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Before you enable IPsec authentication on an OSPFv3 area, you must first enable OSPFv3 globally on the router. Configure the same authentication policy (same SPI and key) on each interface in an OSPFv3 link.

An SPI number must be unique to one IPsec security policy (authentication or encryption) on the router.

If you have enabled IPsec encryption in an OSPFv3 area with the `area encryption` command, you cannot use the `area authentication` command in the area at the same time.

The configuration of IPsec authentication on an interface-level takes precedence over an area-level configuration. If you remove an interface configuration, an area authentication policy that has been configured is applied to the interface.

area encryption

Configure an IPsec encryption policy for OSPFv3 packets in an OSPFv3 area.

Syntax

```
area area-id encryption ipsec spi number esp encryption-
algorithm [key-encryption-type] key authentication-algorithm
[key-encryption-type] key | null
```

To remove an IPsec encryption policy from an interface, use the `no area area-id encryption spi number` command.

Parameters

area *area-id*	Area for which OSPFv3 traffic is to be encrypted. For *area-id*, enter a number. The range is from 0 to 4294967295.
ipsec spi *number*	Security Policy index (SPI) value that identifies an IPsec security policy. The range is from 256 to 4294967295.
esp encryption-algorithm	Encryption algorithm used with ESP. Valid values are: 3DES, DES, AES-CBC, and NULL. For AES-CBC, only the AES-128 and AES-192 ciphers are supported.

key-encryption-algorithm	(OPTIONAL) Specifies if the key is encrypted. Valid values: 0 (key is not encrypted) or 7 (key is encrypted).
key	Text string used in encryption. The required lengths of a non-encrypted or encrypted key are: 3DES - 48 or 96 hex digits; DES - 16 or 32 hex digits; AES-CBC -32 or 64 hex digits for AES-128 and 48 or 96 hex digits for AES-192.
authentication-algorithm	Specifies the authentication algorithm to use for encryption. Valid values are `MD5` or `SHA1`.
key-encryption-type	(OPTIONAL) Specifies if the authentication key is encrypted. Valid values: 0 (key is not encrypted) or 7 (key is encrypted).
key	Text string used in authentication. For MD5 authentication, the key must be 32 hex digits (non-encrypted) or 64 hex digits (encrypted). For SHA-1 authentication, the key must be 40 hex digits (non-encrypted) or 80 hex digits (encrypted).
null	Causes an encryption policy configured for the area to not be inherited on the interface.

Defaults Not configured.

Command Modes ROUTER OSPFv3

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Before you enable IPsec encryption on an OSPFv3 interface, first enable OSPFv3 globally on the router. Configure the same encryption policy (same SPI and keys) on each interface in an OSPFv3 link.

An SPI value must be unique to one IPsec security policy (authentication or encryption) on the router.

When you configure encryption for an OSPFv3 area with the `area encryption` command, you enable both IPsec encryption and authentication. However, when you enable authentication on an area with the `area authentication` command, you do not enable encryption at the same time.

If you have enabled IPsec authentication in an OSPFv3 area with the `area authentication` command, you cannot use the `area encryption` command in the area at the same time.

The configuration of IPsec encryption on an interface-level takes precedence over an area-level configuration. If you remove an interface configuration, an area encryption policy that has been configured is applied to the interface.

clear ipv6 ospf process

Reset an OSPFv3 router process without removing or re-configuring the process.

Syntax

```
clear ipv6 ospf process
```

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

debug ipv6 ospf bfd

Display debug information and interface types for BFD on OSPF IPv6 packets.

Syntax

```
[no] debug ipv6 ospf bfd [interface]
```

To cancel the debug command, use the `no debug ipv6 ospf` command.

Parameters

interface (OPTIONAL) Enter one of the following keywords and slot/port or number information:

- For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
- For a tunnel interface, enter the keyword `tunnel` then a number. The range is from 1 to 16383.

- For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

Command Modes EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information The following section describes the command fields.

Lines Beginning With or Including	Description
OSPFv3...	Debugging is on for all OSPFv3 packets and all interfaces.
05:21:01	Displays the time stamp.
Sending Ver:3	Sending OSPF3 version..

Example

```
Dell(conf-if-te-0/2)#do debug ipv6 ospf bfd te 0/2
OSPFv3 bfd related debugging is on for TenGigabitEthernet 0/2
00:59:26 : OSPFv3INFO: Received Interface mode bfd config
command on interface Te 0/2 Enable 1, interval 0, min_rx 0,
Multiplier 0, role 0, Disable 0
00:59:26 : OSPFv3INFO: Enabling BFD on interface Te 0/2 Cmd
Add Session
00:59:27 : OSPFv3INFO: Enabling BFD for NBRIP
fe80:0000:0000:0000:0201:e8ff:fe8b:7720
00:59:27 : OSPFv3INFO: Completed Enabling BFD on interface Te
0/2
00:59:27 : OSPFv3INFO: Completed Interface mode BFD
configuration on Te 0/2!!
00:59:27 : OSPFv3INFO: Enabling BFD for NBRIP
fe80:0000:0000:0000:0201:e8ff:fe8b:7720
00:59:27 : OSPFv3INFO: Ospf3_register_bfd ospf key 27648
00:59:27 : OSPFv3INFO: OSPFV3 Enabling BFD for NBRIP
fe80:0000:0000:0000:0201:e8ff:fe8b:7720 Interface Te 0/2
IfIndex 34145282
00:59:27 : OSPFv3INFO: BFD parameters interval 100 min_rx 100
mult 3 role active
00:59:27 : OSPFv3INFO: BFD parameters interval 100 min_rx 100
mult 3 role active
00:59:27 : OSPFv3INFO: Completed Enabling BFD for NBRIP
fe80:0000:0000:0000:0201:e8ff:fe8b:7720
Aug 25 11:19:59: %STKUNIT0-M:CP %BFDMGR-1-BFD_STATE_CHANGE:
Changed session state to Init for neighbor fe80::201:e8ff:fe8b:
7720 on interface Te 0/2 (diag: NBR_DN)
Aug 25 11:20:00: %STKUNIT0-M:CP %BFDMGR-1-BFD_STATE_CHANGE:
Changed session state to Up for neighbor fe80::201:e8ff:fe8b:
7720 on interface Te 0/2 (diag: NO_DIAG)
00:59:45 : OSPFv3INFO: OSPFV3 got BFD msg
00:59:45 : OSPFv3INFO: Bfd Msg Type Up for interface Te 0/2
00:59:45 : OSPFv3INFO: OSPFV3 updating NBR state
```

debug ipv6 ospf

Display debug information and interface types on OSPF IPv6 packets or events.

Syntax

```
debug ipv6 ospf {packet | events} [interface]
```

Parameters

interface	(OPTIONAL) Enter one of the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a Port Channel interface, enter the keyword `port-channel` then a number. The range is 1 to 128. • For a tunnel interface, enter the keyword `tunnel` then a number. The range is 1 to 16383. • For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

Command Modes

EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

default-information originate

Configure the system to generate a default external route into an OSPFv3 routing domain.

Syntax

```
default-information originate [always] [metric metric-value]
[metric-type type-value] [route-map map-name]
```

To return to the default values, use the `no default-information originate` command.

Parameters

always	(OPTIONAL) Enter the keyword `always` to specify that default route information must always be advertised.
metric *metric-value*	(OPTIONAL) Enter the keyword `metric` then a number to configure a metric value for the route. The range is from 1 to 16777214.
metric-type *type-value*	(OPTIONAL) Enter the keywords `metric-type` then an OSPFv3 link state type of 1 or 2 for default routes. The values are:

		- 1 = Type 1 external route - 2 = Type 2 external route
	route-map *map-name*	(OPTIONAL) Enter the keywords `route-map` then the name of an established route map.
Defaults	Disabled.	
Command Modes	ROUTER OSPFv3	
Command History	**Version 9.2(0.0)**	Introduced on the MXL 10/40GbE Switch IO Module.

graceful-restart grace-period

Enable OSPFv3 graceful restart globally by setting the grace period (in seconds) that an OSPFv3 router's neighbors continues to advertise the router as adjacent during a graceful restart.

Syntax

`graceful-restart grace-period` *`seconds`*

To disable OSPFv3 graceful restart, enter `no graceful-restart grace-period`.

Parameters

seconds	Time duration, in seconds, that specifies the duration of the restart process before OSPFv3 terminates the process. The range is from 40 to 1800 seconds.

Defaults

OSPFv3 graceful restart is disabled and functions in a helper-only role.

Command Modes

ROUTER OSPFv3

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

By default, OSPFv3 graceful restart is disabled and functions only in a helper role to help restarting neighbor routers in their graceful restarts when it receives a Grace LSA.

To enable OSPFv3 graceful restart, enter the ipv6 router ospf command to enter OSPFv3 configuration mode and then configure a grace period using the graceful-restart grace-period command. The grace period is the length of time that OSPFv3 neighbors continue to advertise the restarting router as though it is fully adjacent. When graceful restart is enabled (restarting role), an OSPFv3 restarting expects its OSPFv3 neighbors to help when it restarts by not advertising the broken link.

When you enable the helper-reject role on an interface with the ipv6 ospf graceful-restart helper-reject command, you reconfigure OSPFv3 graceful restart to function in a “restarting-only” role. In a “restarting-only” role, OSPFv3 does not participate in the graceful restart of a neighbor.

graceful-restart mode

Specify the type of events that trigger an OSPFv3 graceful restart.

Syntax

`graceful-restart mode {planned-only | unplanned-only}`

To disable graceful restart mode, enter `no graceful-restart mode`.

Parameters

planned-only	(OPTIONAL) Enter the keywords `planned-only` to indicate graceful restart is supported in a planned restart condition only.
unplanned-only	(OPTIONAL) Enter the keywords `unplanned-only` to indicate graceful restart is supported in an unplanned restart condition only.

Defaults

OSPFv3 graceful restart supports both planned and unplanned failures.

Command Modes

ROUTER OSPFv3

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

OSPFv3 graceful restart supports planned-only and/or unplanned-only restarts. The default is support for both planned and unplanned restarts.

- A planned restart occurs when you enter the `redundancy force-failover rpm` command to force the primary RPM to switch to the backup RPM. During a planned restart, OSPF sends out a Type-11 Grace LSA before the system switches over to the backup RPM.
- An unplanned restart occurs when an unplanned event causes the active RPM to switch to the backup RPM, such as when an active process crashes, the active RPM is removed, or a power failure happens. During an unplanned restart, OSPF sends out a Grace LSA when the backup RPM comes online.

By default, both planned and unplanned restarts trigger an OSPFv3 graceful restart. Selecting one or the other mode restricts OSPFv3 to the single selected mode.

ipv6 ospf area

Enable IPv6 OSPF on an interface.

Syntax	`ipv6 ospf` *`process id`* `area` *`area id`* To disable OSPFv6 routing for an interface, use the `no ipv6 ospf` *`process-id`* `area` *`area-id`* command.
Parameters	
Defaults	none
Command Modes	INTERFACE
Command History	Version 9.2(0.0) — Introduced on the MXL 10/40GbE Switch IO Module.

Parameters:

process-id	Enter the process identification number.
area *area-id*	Specify the OSPF area. The range is from 0 to 65535.

Command History:

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

ipv6 ospf authentication

Enable IPv6 OSPF on an interface.

Syntax

`ipv6 ospf authentication {null |` *`ipsec spi number`* `{MD5 | SHA1} [`*`key-encryption-type`*`]` *`key`*`}}`

To remove an IPsec authentication policy from an interface, use the `no ipv6 ospf authentication spi number` command.

To remove null authentication on an interface to allow the interface to inherit the authentication policy configured for the OSPFv3 area, use the `no ipv6 ospf authentication null` command.

Parameters

null	Causes an authentication policy configured for the area to not be inherited on the interface.
ipsec spi number	Security Policy index (SPI) value that identifies an IPsec security policy. The range is from 256 to 4294967295.
MD5 | SHA1	Authentication type: Message Digest 5 (MD5) or Secure Hash Algorithm 1 (SHA-1).
key-encryption-type	(OPTIONAL) Specifies if the key is encrypted. Valid values: 0 (key is not encrypted) or 7 (key is encrypted).
key	Text string used in authentication.

For MD5 authentication, the key must be 32 hex digits (non-encrypted) or 64 hex digits (encrypted).

For SHA-1 authentication, the key must be 40 hex digits (non-encrypted) or 80 hex digits (encrypted).

Defaults Not configured.

Command Modes INTERFACE

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Before you enable IPsec authentication on an OSPFv3 interface, first enable IPv6 unicast routing globally, configure an IPv6 address and enable OSPFv3 on the interface, and assign the interface to an area.

An SPI value must be unique to one IPsec security policy (authentication or encryption) on the router. Configure the same authentication policy (same SPI and key) on each OSPFv3 interface in a link.

ipv6 ospf bfd all-neighbors

Establish BFD sessions with all OSPFv3 neighbors on a single interface or use non-default BFD session parameters.

Syntax

```
ipv6 ospf bfd all-neighbors [disable | [interval interval
min_rx min_rx multiplier value role {active | passive}]]
```

To disable all BFD sessions on an OSPFv3 interface implicitly, use the `no ipv6 ospf bfd all-neighbors disable` command.

Parameters

disable	(OPTIONAL) Enter the keyword `disable` to disable BFD on this interface.
interval *milliseconds*	(OPTIONAL) Enter the keyword `interval` to specify non-default BFD session parameters beginning with the transmission interval. The range is from 50 to 1000. The default is 100.
min_rx *milliseconds*	Enter the keywords `min_rx` to specify the minimum rate at which the local system would like to receive control packets from the remote system. The range is from 50 to 100. The default is **100**.
multiplier *value*	Enter the keyword `multiplier` to specify the number of packets that must be missed in order to declare a session down. The range is from 3 to 50. The default is **3**.

role [active | passive]	Enter the role that the local system assumes: • **active** — The active system initiates the BFD session. Both systems can be active for the same session. • **passive** — The passive system does not initiate a session. It only responds to a request for session initialization from the active system. The default is **Active**.

Defaults

See Parameters.

Command Modes

INTERFACE

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

This command provides the flexibility to fine-tune the timer values based on individual interface needs when you configure the `ipv6 ospf bfd` command in CONFIGURATION mode. Any timer values specified with this command overrides timers set using the `bfd all-neighbors` command. Using the `no` form of this command does not disable BFD if you configured BFD in CONFIGURATION mode.

To disable BFD on a specific interface while BFD is configured in CONFIGURATION mode, use the keyword `disable`.

ipv6 ospf cost

Explicitly specify the cost of sending a packet on an interface.

Syntax

```
ipv6 ospf interface-cost
```

Parameters

interface-cost	Enter a unsigned integer value expressed as the link-state metric. The range is from 1 to 65535.

Defaults

Default cost based on the bandwidth.

Command Modes

INTERFACE

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

In general, the path cost is calculated as:

10^8 / bandwidth

Using this formula, the default path cost is calculated as:

- GigabitEthernet—Default cost is 1
- TenGigabitEthernet—Default cost is 1
- FortygigEthernet — Default cost is 1
- Ethernet—Default cost is 10

ipv6 ospf dead-interval

Set the time interval since the last hello-packet was received from a router. After the time interval elapses, the neighboring routers declare the router down.

Syntax `ipv6 ospf dead-interval seconds`

Parameters

seconds	Enter the time interval in seconds. The range is from 1 to 65535 seconds.

Defaults 40 seconds (Ethernet).

Command Modes INTERFACE

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information By default, the dead interval is four times longer than the default `ipv6 ospf hello-interval` command.

ipv6 ospf encryption

Configure an IPsec encryption policy for OSPFv3 packets on an IPv6 interface.

Syntax

```
ipv6 ospf encryption {null | ipsec spi number esp encryption-algorithm [key-encryption-type] key athentication-algorithm [key-encryption-type] key}}
```

To remove an IPsec encryption policy from an interface, use the `no ipv6 ospf encryption spi number` command.

To remove null authentication on an interface to allow the interface to inherit the authentication policy configured for the OSPFv3 area, use the `no ipv6 ospf encryption null` command.

Parameters

null	Causes an encryption policy configured for the area to not be inherited on the interface.
ipsec spi number	Security Policy index (SPI) value that identifies an IPsec security policy. The range is from 256 to 4294967295.
esp *encryption-algorithm*	Encryption algorithm used with ESP. Valid values are: 3DES, DES, AES-CBC, and NULL. For AES-CBC, only the AES-128 and AES-192 ciphers are supported.
key-encryption-type	(OPTIONAL) Specifies if the key is encrypted. Valid values: 0 (key is not encrypted) or 7 (key is encrypted).
key	Text string used in authentication. The required lengths of a non-encrypted or encrypted key are: 3DES - 48 or 96 hex digits; DES - 16 or 32 hex digits; AES-CBC -32 or 64 hex digits for AES-128 and 48 or 96 hex digits for AES-192.
authentication-algorithm	Specifies the authentication algorithm to use for encryption. Valid values are `MD5` or `SHA1`.
key-encryption-type	(OPTIONAL) Specifies if the authentication key is encrypted. Valid values: 0 (key is not encrypted) or 7 (key is encrypted).
key	Text string used in authentication. For MD5 authentication, the key must be 32 hex digits (non-encrypted) or 64 hex digits (encrypted). For SHA-1 authentication, the key must be 40 hex digits (non-encrypted) or 80 hex digits (encrypted).

Defaults Not configured.

Command Modes INTERFACE

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information	Before you enable IPsec encryption on an OSPFv3 interface, first enable IPv6 unicast routing globally, configure an IPv6 address and enable OSPFv3 on the interface, and assign the interface to an area. An SPI value must be unique to one IPsec security policy (authentication or encryption) on the router. Configure the same encryption policy (same SPI and key) on each OSPFv3 interface in a link.

ipv6 ospf graceful-restart helper-reject

Configure an OSPFv3 interface to not act upon the Grace LSAs that it receives from a restarting OSPFv3 neighbor.

Syntax

```
ipv6 ospf graceful-restart helper-reject
```

To disable the helper-reject role, use the `no ipv6 ospf graceful-restart helper-reject` command.

Defaults	The helper-reject role is not configured.
Command Modes	INTERFACE
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Command	By default, OSPFv3 graceful restart is disabled and functions only in a helper role to help restarting neighbor routers in their graceful restarts when it receives a Grace LSA. When configured in a helper-reject role, an OSPFv3 router ignores the Grace LSAs that it receives from a restarting OSPFv3 neighbor. The graceful-restart role command is not supported in OSPFv3. When you enable the helper-reject role on an interface, you reconfigure an OSPFv3 router to function in a “restarting-only” role.

ipv6 ospf hello-interval

Specify the time interval between the hello packets sent on the interface.

Syntax

```
ipv6 ospf hello—interval seconds
```

Parameters

seconds	Enter the time interval in seconds as the time between hello packets. The range is from 1 to 65525 seconds.

Defaults	10 seconds (Ethernet).
Command Modes	INTERFACE
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	The time interval between hello packets must be the same for routers in a network.

ipv6 ospf priority

To determine the Designated Router for the OSPFv3 network, set the priority of the interface.

Syntax

```
ipv6 ospf priority number
```

To return to the default time interval, use the `no ipv6 ospf priority` command.

Parameters

number	Enter the number as the priority. The range is from 1 to 255.

Defaults	1
Command Modes	INTERFACE
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Setting a priority of 0 makes the router ineligible for election as a Designated Router or Backup Designated Router.

Use this command for interfaces connected to multi-access networks, not point-to-point networks.

ipv6 router ospf

Enable OSPF for IPv6 router configuration.

Syntax

```
ipv6 router ospf process-id
```

To exit OSPF for IPv6, use the `no ipv6 router ospf process-id` command.

Parameters

process-id	Enter the process identification number. The range is from 1 to 65535.

Defaults

none

Command Modes

CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

maximum-paths

Enable the software to forward packets over multiple paths.

Syntax

`maximum-paths number`

To disable packet forwarding over multiple paths, use the `no maximum-paths` command.

Parameters

number	Specify the number of paths. The range is from 1 to 64. The default is **8** paths.

Defaults

4

Command Modes

ROUTER OSPF for OSPFv3

Command History

Version 9.2(0.0)	Added support for OSPFv3.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

passive-interface

Disable (suppress) sending routing updates on an interface.

Syntax

`passive—interface {default | interface}`

To enable sending routing updates on an interface, use the `no passive-interface interface` command.

To return all OSPF interfaces (current and future) to active, use the `no passive-interface default` command.

Parameters	**Default**	Enter the keyword `default` to make all OSPF interfaces (current and future) passive.
	interface	Enter the following keywords and slot/port or number information: • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

Command Modes

ROUTER OSPF for OSPFv2

ROUTER OSPFv3 for OSPFv3

Command History

Version 9.2(0.0)	Added support for OSPFv3.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

By default, no interfaces are *passive*. Routing updates are sent to all interfaces on which the routing protocol is enabled.

If you disable the sending of routing updates on an interface, the particular address prefix continues to be advertised to other interfaces, and updates from other routers on that interface continue to be received and processed.

OSPFv3 for IPv6 routing information is not sent or received through the specified router interface. The specified interface address appears as a stub network in the OSPFv3 for IPv6 domain.

redistribute

Redistribute information from another routing protocol into OSPFv3 throughout the OSPF process.

Syntax

`redistribute {bgp as number}{connected | static}[metric metric-value | metric-type type-value] [route-map map-name] [tag tag-value]`

To disable redistribution, use the `no redistribute {connected | static}` command.

Parameters

bgp *as number*	Enter the keyword `bgp` then the autonomous system number. The range is from 1 to 65535.
connected	Enter the keyword `connected` to redistribute routes from physically connected interfaces.
static	Enter the keyword `static` to redistribute manually configured routes.
metric *metric-value*	Enter the keyword `metric` then the metric value. The range is from 0 to 16777214. The default is **20**.
metric-type *type-value*	(OPTIONAL) Enter the keywords `metric-type` then the OSPFv3 link state type of 1 or 2 for default routes. The values are: • 1 for a type 1 external route • 2 for a type 2 external route The default is **2**.
route-map *map-name*	(OPTIONAL) Enter the keywords `route-map` then the name of an established route map. If the route map is not configured, the default is **deny** (to drop all routes).
tag *tag-value*	(OPTIONAL) Enter the keyword `tag` to set the tag for routes redistributed into OSPFv3. The range is from 0 to 4294967295 The default is **0**.

Defaults

Not configured.

Command Modes

ROUTER OSPF for OSPFv2

ROUTER OSPFv3 for OSPFv3

Command History

Version 9.2(0.0)	Added support for OSPFv3.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To redistribute the default route (x:x:x:x::x), use the `default-information originate` command.

Related Commands

default-information originate — generates a default route into the OSPF routing domain.

router-id

Designate a fixed router ID.

Syntax

`router-id ip-address`

To return to the previous router ID, use the `no router-id ip-address` command.

Parameters

ip-address	Enter the router ID in the dotted decimal format.

Defaults

The router ID is selected automatically from the set of IPv4 addresses configured on a router.

Command Modes

ROUTER OSPFv3 for OSPFv3

Command History

Version 9.2(0.0)	Added support for OSPFv3.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

You can configure an arbitrary value in the IP address for each router. However, each router ID must be unique.

If this command is used on an OSPFv3 process that is already active (has neighbors), all the neighbor adjacencies are brought down immediately and new sessions are initiated with the new router ID.

Example

```
Dell(conf)#router ospf 100
Dell(conf-router_ospf)#router-id 1.1.1.1
Changing router-id will bring down existing OSPF adjacency [y/
n]:

Dell(conf-router_ospf)#show config
!
router ospf 100
router-id 1.1.1.1
Dell(conf-router_ospf)#no router-id
Changing router-id will bring down existing OSPF adjacency [y/
n]:
Dell#
```

show crypto ipsec policy

Display the configuration of IPsec authentication and encryption policies.

Syntax **show crypto ipsec policy** `[name name]`

Parameters

name *name*	(OPTIONAL) Displays configuration details about a specified policy.

Defaults none

Command Modes

EXEC

EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The `show crypto ipsec policy` command output displays the AH and ESP parameters configured in IPsec security policies, including the SPI number, keys, and algorithms used.

When configured in a helper-reject role, an OSPFv3 router ignores the Grace LSAs that it receives from a restarting OSPFv3 neighbor.

show crypto ipsec sa ipv6

Display the IPsec security associations (SAs) used on OSPFv3 interfaces.

Syntax `show crypto ipsec sa ipv6 [interface interface]`

Parameters

interface *interface*	(OPTIONAL) Displays information about the SAs used on a specified OSPFv3 interface, where *interface* is one of the following values: • For a 1-Gigabit Ethernet interface, enter `GigabitEthernet` then the slot/part number. • For a Port Channel interface, enter `port-channel` then the port channel number. • For a 10-Gigabit Ethernet interface, enter `TenGigabitEthernet` then the slot/port number. • For a 40–Gigabit Ethernet interface, enter `fortyGigE` then the slot/port number. • For a VLAN interface, enter `vlan vlan-id`. The valid VLAN IDs range is from 1 to 4094.

Defaults	none
Command Modes	EXEC EXEC Privilege
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	The `show crypto ipsec sa ipv6` command output displays security associations set up for OSPFv3 links in IPsec authentication and encryption policies on the router.

show ipv6 ospf database

Display information in the OSPFv3 database, including link-state advertisements (LSAs).

Syntax	`show ipv6 ospf database [database-summary | grace-lsa]`	
Parameters	database-summary	(OPTIONAL) Enter the keywords `database-summary` to view a summary of database LSA information.
	grace-lsa	(OPTIONAL): Enter the keywords `grace-lsa` to display the Type-11 Grace LSAs sent and received on an OSPFv3 router.
Defaults	none	
Command Modes	EXEC EXEC Privilege	
Command History	**Version 9.2(0.0)**	Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	The `show crypto ipsec sa ipv6` command output displays security associations set up for OSPFv3 links in IPsec authentication and encryption policies on the router.	

show ipv6 ospf interface

View OSPFv3 interface information.

Syntax

```
show ipv6 ospf [interface]
```

Parameters

interface	(OPTIONAL) Enter one of the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` and the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` and the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` and the slot/port information. • For a Port Channel interface, enter the keywords `port-channel` and a number. The range is from 1 to 128. • For a Tunnel interface, enter the keywords `tunnel` and a number. The range is from 1 to 16383. • For a VLAN, enter the keyword `vlan` and a number from 1 to 4094.

Defaults

none

Command Modes

EXEC

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

If you enable BFD at the global level, *show ipv6 ospf interface* shows the BFD provisioning.

If you enable BFD at the interface level, *show ipv6 ospf interface* shows the BFD interval timers.

Example

```
Dell#show ipv6 ospf interface gigabitethernet 1/0

GigabitEthernet 1/0 is up, line protocol is up
  Link Local Address fe80::201:e8ff:fe17:5bbd, Interface ID
67420217
  Area 0, Process ID 1, Instance ID 0, Router ID 11.1.1.1
  NetworkType BROADCAST, Cost: 1, Passive: No
  Transmit Delay is 100 sec, State DR, Priority 1
  Interface is using OSPF global mode BFD configuration.
  Designated router on this network is 11.1.1.1 (local)
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 1,
Retransmit 5

Dell#
```

show ipv6 ospf neighbor

Display the OSPF neighbor information on a per-interface basis.

Syntax	`show ipv6 ospf neighbor [interface]`

Parameters

interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is 1 to 128. • For a VLAN, enter the keyword `vlan` then the VLAN ID. The range is 1 to 4094.

Defaults	none
Command Modes	EXEC EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

38

Policy-based Routing (PBR)

Policy-based routing (PBR) allows you to apply routing policies to specific interfaces. To enable PBR, create a redirect list and apply it to the interface. After the redirect list is applied to the interface, all traffic passing through the interface is subject to the rules defined in the redirect list. PBR is supported by the Dell Networking operating software (OS) in MXL platform.

You can apply PBR to physical interfaces and logical interfaces (such as a link aggregation group [LAG] or virtual local area network [VLAN]). Trace lists and redirect lists do not function correctly when you configure both in the same configuration.

NOTE: Apply PBR to Layer 3 interfaces only.

description

Add a description to this redirect list.

Syntax	`description {`*`description`*`}` To remove the description, use the `no description {`*`description`*`}` command.
Parameters	*description* — Enter a description to identify the IP redirect list (80 characters maximum).
Defaults	none
Command Modes	REDIRECT-LIST
Command History	Version 9.4(0.0) — Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	ip redirect-list – enables an IP Redirect List.

ip redirect-group

Apply a redirect list (policy-based routing) on an interface. You can apply multiple redirect lists to an interface by entering this command multiple times.

Syntax	`ip redirect-group `*`redirect-list-name`*

To remove a redirect list from an interface, use the `no ip redirect-group` *`name`* command.

Parameters

redirect-list-name	Enter the name of a configured redirect list.

Defaults none

Command Modes INTERFACE (conf-if-vl-)

Command History

Version 9.4(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.
Version 8.4.2.1	Introduced on the C-Series and S-Series.
Version 8.4.2.0	Introduced on the E-Series TeraScale.
Version 7.4.2.0	Added support for LAG and VLAN interfaces.
pre-Version 7.7.1.0	Introduced on the E-Series ExaScale.

Usage Information

You can apply any number of redirect-groups to an interface. A redirect list can contain any number of configured rules. These rules includes the next-hop IP address where the incoming traffic is to be redirected.

If the next hop address is reachable, traffic is forwarded to the specified next hop. Otherwise, the normal routing table is used to forward traffic. When a redirect-group is applied to an interface and the next-hop is reachable, the rules are added into the PBR CAM region. When incoming traffic hits an entry in the CAM, the traffic is redirected to the corresponding next-hop IP address specified in the rule.

NOTE: Apply the redirect list to physical, VLAN, or LAG interfaces only.

Related Commands

- show cam pbr – displays the content of the PBR CAM.
- show ip redirect-list – displays the redirect-list configuration.

ip redirect-list

Configure a redirect list and enter REDIRECT-LIST mode.

Syntax

`ip redirect-list` *`redirect-list-name`*

To remove a redirect list, use the `no ip redirect-list` command.

Parameters

redirect-list-name	Enter the name of a redirect list.

Defaults none

Command Modes CONFIGURATION

Command History

Version 9.4.0.0	Introduced on the MXL 10/40GbE Switch IO Module.
Version 8.4.2.1	Introduced on the C-Series and S-Series.
Version 8.4.2.0	Introduced on the E-Series TeraScale.
Version 6.5.3.0	Introduced on the E-Series ExaScale.

permit

Configure a rule for the redirect list.

Syntax

`permit {ip-protocol-number | protocol-type} {source mask | any | host ip-address} {destination mask | any | host ip-address} [bit] [operators]`

To remove the rule, use one of the following:

- If you know the filter sequence number, use the `no seq sequence-number syntax` command.
- You can also use the `no permit {ip-protocol-number | protocol-type} {source mask | any | host ip-address} {destination mask | any | host ip-address} [bit] [operators]` command.

Parameters

ip-protocol-number	Enter a number from 0 to 255 for the protocol identified in the IP protocol header.
protocol-type	Enter one of the following keywords as the protocol type: • `icmp` for internet control message protocol • `ip` for any internet protocol • `tcp` for transmission control protocol • `udp` for user datagram protocol
source	Enter the IP address of the network or host from which the packets were sent.
mask	Enter a network mask in /prefix format (/x).
any	Enter the keyword `any` to specify that all traffic is subject to the filter.
host *ip-address*	Enter the keyword `host` then the IP address to specify a host IP address.
destination	Enter the IP address of the network or host to which the packets are sent.

bit	(OPTIONAL) For the TCP protocol type only, enter one or a combination of the following TCP flags: • `ack` = acknowledgement • `fin` = finish (no more data from the user) • `psh` = push function • `rst` = reset the connection • `syn` = synchronize sequence number • `urg` = urgent field
operator	(OPTIONAL) For TCP and UDP parameters only. Enter one of the following logical operand: • `eq` = equal to • `neq` = not equal to • `gt` = greater than • `lt`= less than • `range` = inclusive range of ports (you must specify two ports for the `port`command parameter.)

Defaults none

Command Modes REDIRECT-LIST

Command History

Version 9.4(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.
Version 8.4.2.1	Introduced on the C-Series and S-Series.
Version 8.4.2.0	Introduced on the E-Series TeraScale.
Version 7.5.1.0	Introduced on the E-Series ExaScale.

redirect

Configure a rule for the redirect list.

Syntax

```
redirect {ip-address | slot/port} {ip-protocol-number |
protocol-type [bit]} {source mask | any | host ip-address}
{destination mask | any | host ip-address} [operator]
```

To remove this filter, use one of the following:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- You can also use the `no redirect {ip-address | slot/port} {ip-protocol-number [bit] | protocol-type} {source mask | any |`

`host ip-address} {destination mask | any | host ip-address}` `[operator]` command.

Parameters

ip-address	Enter the IP address of the forwarding router.
slot/port	Enter the keyword `slot / port` followed by the slot/port information.
ip-protocol-number	Enter a number from 0 to 255 for the protocol identified in the IP protocol header.
protocol-type	Enter one of the following keywords as the protocol type: • `icmp` for internet control message protocol • `ip` for any internet protocol • `tcp` for transmission control protocol • `udp` for user datagram protocol
bit	(OPTIONAL) For the TCP protocol type only, enter one or a combination of the following TCP flags: • `ack` = acknowledgement • `fin` = finish (no more data from the user) • `psh` = push function • `rst` = reset the connection • `syn` = synchronize sequence number • `urg` = urgent field
source	Enter the IP address of the network or host from which the packets were sent.
mask	Enter a network mask in /prefix format (/x).
any	Enter the keyword `any` to specify that all traffic is subject to the filter.
host *ip-address*	Enter the keyword `host` then the IP address to specify a host IP address.
destination	Enter the IP address of the network or host to which the packets are sent.
operator	(OPTIONAL) For TCP and UDP parameters only. Enter one of the following logical operand: • `eq` = equal to • `neq` = not equal to • `gt` = greater than • `lt` = less than • `range` = inclusive range of ports (you must specify two ports for the`port` command parameter.)

Defaults	none
Command Modes	REDIRECT-LIST

Command History

Version 9.4.0.0	Introduced on the MXL 10/40GbE Switch IO Module.
Version 8.4.2.1	Introduced on the C-Series.
Version 8.4.2.0	Introduced on the E-Series TeraScale.

seq

Configure a filter with an assigned sequence number for the redirect list.

Syntax

```
seq sequence-number {permit | redirect {ip-address}} {ip-
protocol-number | protocol-type} {source mask | any | host ip-
address} {destination mask | any | host ip-address} [bit]
[operator]{source-port source-port| source-port-range start-
port - end-port} {destination-port destination-port|
destination-port-range start-port - end-port}
```

To delete a filter, use the `no seq sequence-number` command.

Parameters

sequence-number	Enter a number from 1 to 65535.
permit	Enter the keyword `permit` assign the sequence to the permit list.
redirect	Enter the keyword `redirect` to assign the sequence to the redirect list.
ip-address	Enter the `IP address` of the forwarding router.
ip-protocol-number	Enter the keyword `ip-protocol-number` then the number from 0 to 255 for the protocol identified in the IP protocol header.
protocol-type	Enter one of the following keywords as the protocol type: • `icmp` for internet control message protocol • `ip` for any internet protocol • `tcp` for transmission control protocol • `udp` for user datagram protocol
source	Enter the IP address of the network or host from which the packets were sent.
mask	Enter a network mask in /prefix format (/x).

any	Enter the keyword `any` to specify that all traffic is subject to the filter.
host *ip-address*	Enter the keyword `host` then the IP address to specify a host IP address.
destination	Enter the IP address of the network or host to which the packets are sent.
bit	(OPTIONAL) For the TCP protocol type only, enter one or a combination of the following TCP flags: • `ack` = acknowledgement • `fin` = finish (no more data from the user) • `psh` = push function • `rst` = reset the connection • `syn` = synchronize sequence number • `urg` = urgent field
operator	(OPTIONAL) For the TCP and UDP parameters only. Enter one of the following logical operand: • `eq` = equal to • `neq` = not equal to • `gt` = greater than • `lt`= less than • `range` = inclusive range of ports (you must specify two ports for the port command parameter.)
source port	Enter the keywords `source-port` then the port number to be matched in the ACL rule in the ICAP rule
destination-port	Enter the keywords `destination-port` then the port number to be matched in the ACL rule in the ICAP rule.
source-port-range	Enter the keywords `Source-port-range` then the range of the start port to end port to be matched in the ACL rule in the ICAP rule.
destination-port-range	Enter the keywords `destination-port-range` then the range of the start port to end port to be matched in the ACL rule in the ICAP rule.

Defaults	none	
Command Modes	REDIRECT-LIST	
Command History	Version 9.4(0.0)	Added support for removing the Sonet interface on the MXL 10/40GbE Switch IO Module.

show cam pbr

Display the PBR CAM content.

Syntax `show cam pbr {[interface interface] | stack—unit slot-number port-set number]} [summary]`

Parameters

interface *interface*	Enter the keyword `interface` then the name of the interface.
stack–unit *number*	Enter the keyword `stack-unit` then the slot number. The range is from 0 to 11 .
port-set *number*	Enter the keywords `port-set` then the port-pipe number. The range is from 0 to 1.
summary	Enter the keyword `summary` to view only the total number of CAM entries.

Defaults none

Command Modes EXEC

Command History

Version 9.4(0.0)	Added support for removing the Sonet interface on the MXL 10/40GbE Switch IO Module.
Version 7.4.1.0	Introduced.

Usage Information The `show cam pbr` command displays the PBR CAM content.

Example

```
Dell#show cam pbr stack-unit 0 po 0

TCP Flag: Bit 5 - URG, Bit 4 - ACK, Bit 3 - PSH, Bit 2 - RST,
Bit 1 - SYN, Bit 0 - FIN

Cam   Port VlanID Proto Tcp   Src   Dst
SrcIp
DstIp                           Next-hop          Egress
Index                   Flag  Port
Port
       MAC               Port
---------------------------------------------------------------
---------------------------------------------------------------
------------
00000 5    N/A    IP    0x0   0     0
22.22.2.22/32
33.33.3.0/24                    00:01:e8:8a:fd:76   0/0
00001 5    N/A    145   0x0   0     0
0.0.0.0/0
44.4.4.4/32                     00:01:e8:8a:fd:76 Vl 100(0/1)
00002 5    N/A    TCP   0x0   0     0
55.1.3.0/24
66.6.6.6/32                     00:01:e8:8a:fd:76 Po 128
00003 5    N/A    UDP   0x0   0     0
55.1.3.0/24
66.6.6.6/32                     00:01:e8:8a:fd:76 Po 128
00004 5    N/A    IP    0x0   0     0
```

```
0.0.0.0/0
0.0.0.0/0                        00:01:e8:8a:fd:76 Vl 1020(Po
100)
Dell#
```

Related Commands

- ip redirect-group – applies a redirect group to an interface.
- show ip redirect-list – displays the redirect-list configuration.
- show cam-usage – displays the CAM usage on ACL, router, or switch.

show ip redirect-list

View the redirect list configuration and the interfaces it is applied to.

Syntax

`show ip redirect-list redirect-list-name`

Parameters

redirect-list-name	Enter the name of a configured Redirect list.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.4(0.0)	Added support for removing the Sonet interface on the MXL.
Version 7.4.1.0	Introduced.

Example

```
Dell#show ip redirect-list test_pbr

IP redirect-list test_pbr:
 Defined as:
  seq 5 redirect 1.1.1.2 ip host 22.22.2.22 33.33.3.0/24, Next-
hop reachable (via Te 0/0), ARP resolved
,
  seq 10 redirect 2.1.1.2 145 any host 44.4.4.4, Next-hop
reachable (via Vl 100), ARP resolved
,
  seq 15 redirect 3.1.1.2 tcp 55.1.3.0/24 host 66.6.6.6, Next-
hop reachable (via Po 128), ARP resolved
,
  seq 20 redirect 3.1.1.2 udp 55.1.3.0/24 host 66.6.6.6, Next-
hop reachable (via Po 128), ARP resolved
,
  seq 25 redirect 4.1.1.2 ip any any, Next-hop reachable (via
Vl 1020), ARP resolved
,
 Applied interfaces:
  Te 0/5
Dell#
```

39

PIM-Sparse Mode (PIM-SM)

The protocol-independent multicast (PIM) commands are supported by the Dell Networking Operating System (OS).

This chapter contains the following sections:

- IPv4 PIM-Sparse Mode Commands
- IPv6 PIM-Sparse Mode Commands

IPv4 PIM-Sparse Mode Commands

The following describes the IPv4 PIM-sparse mode (PIM-SM) commands.

clear ip pim rp-mapping

The bootstrap router (BSR) feature uses this command to remove all or particular rendezvous point (RP) advertisement.

Syntax	`clear ip pim rp-mapping rp-address`
Parameters	*rp-address*: (OPTIONAL) Enter the RP address in dotted decimal format (A.B.C.D).
Command Modes	EXEC Privilege
Command History	Version 9.2(0.0): Introduced on the MXL 10/40GbE Switch IO Module.

clear ip pim tib

Clear PIM tree information from the PIM database.

Syntax	`clear ip pim tib [group]`
Parameters	group: (OPTIONAL) Enter the multicast group address in dotted decimal format (A.B.C.D).

Command Modes

EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

If you use this command on a local VLT node, all multicast routes from the local PIM TIB, the entire multicast route table, and all the entries in the data plane are deleted. The local VLT node sends a request to the peer VLT node to download multicast routes learned by the peer. Both local and synced routes are removed from the local VLT node multicast route table. The peer VLT node clears synced routes from the node.

If you use this command on a peer VLT node, only the synced routes are deleted from the multicast route table.

debug ip pim

View IP PIM debugging messages.

Syntax

```
debug ip pim [bsr | events | group | packet [in | out] |
register | state | timer [assert | hello | joinprune |
register]]
```

To disable PIM debugging, use the `no debug ip pim` command or use the `undebug all` to disable all the debugging commands.

Parameters

bsr	(OPTIONAL) Enter the keyword `bsr` to view PIM Candidate RP/BSR activities.
events	(OPTIONAL) Enter the keyword `group` to view PIM messages for a specific group.
group	(OPTIONAL) Enter the keyword `group` to view PIM messages for a specific group.
packet [in | out]	(OPTIONAL) Enter the keyword `packet` to view PIM packets. Enter one of the optional parameters: • `in`: to view incoming packets • `out`: to view outgoing packets
register	(OPTIONAL) Enter the keyword `register` to view PIM register address in dotted decimal format (A.B.C.D).
state	(OPTIONAL) Enter the keyword `state` to view PIM state changes.

timer [assert | hello | joinprune | register]	(OPTIONAL) Enter the keyword `timer` to view PIM timers. Enter one of the optional parameters: • `assert`: to view the assertion timer • `hello`: to view the PIM neighbor keepalive timer • `joinprune`: to view the expiry timer (join/prune timer) • `register`: to view the register suppression timer

Defaults
Disabled.

Command Modes
EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

ip pim bsr-border

Define the border of PIM domain by filtering inbound and outbound PIM-BSR messages per interface.

Syntax
`ip pim bsr-border`

To return to the default value, use the `no ip pim bsr-border` command.

Defaults
Disabled.

Command Modes
INTERFACE

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information
This command is applied to the subsequent PIM-BSR. Existing BSR advertisements are cleaned up by time-out. To clean the candidate RP advertisements, use the `clear ip pim rp-mapping` command.

ip pim bsr-candidate

To join the Bootstrap election process, configure the PIM router.

Syntax
`ip pim bsr-candidate` *`interface`* `[`*`hash-mask-length`*`] [`*`priority`*`]`

To return to the default value, use the `no ip pim bsr-candidate` command.

Parameters

interface	Enter the following keywords and slot/port or number information:

- For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383.
- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

hash-mask-length	(OPTIONAL) Enter the hash mask length. The range is from zero (0) to 32. The default is **30**.
priority	(OPTIONAL) Enter the priority used in Bootstrap election process. The range is from zero (0) to 255. The default is **zero (0)**.

Defaults: Not configured.

Command Modes: CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

ip pim dr-priority

Change the designated router (DR) priority for the interface.

Syntax: `ip pim dr-priority` *`priority-value`*

To remove the DR priority value assigned, use the `no ip pim dr-priority` command.

Parameters

priority-value	Enter a number. Preference is given to larger/higher number. The range is from 0 to 4294967294. The default is 1.

Defaults: **1**

Command Modes: INTERFACE

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information: The router with the largest value assigned to an interface becomes the designated router. If two interfaces contain the same designated router priority value, the interface with the largest interface IP address becomes the designated router.

ip pim join-filter

Permit or deny PIM Join/Prune messages on an interface using an extended IP access list. This command prevents the PIM-SM router from creating state based on multicast source and/or group.

Syntax

`ip pim join-filter` *`ext-access-list`* `{in | out}`

To remove the access list, use the `no ip pim join-filter ext-access-list {in | out}` command.

Parameters

ext-access-list	Enter the name of an extended access list.
in	Enter this keyword to apply the access list to inbound traffic.
out	Enter this keyword to apply the access list to outbound traffic.

Defaults

none

Command Modes

INTERFACE

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell(conf)# ip access-list extended iptv-channels
Dell(config-ext-nacl)# permit ip 10.1.2.3/24 225.1.1.0/24
Dell(config-ext-nacl)# permit ip any 232.1.1.0/24
Dell(config-ext-nacl)# permit ip 100.1.1.0/16 any
Dell(config-if-gi-1/1)# ip pim join-filter iptv-channels in
Dell(config-if-gi-1/1)# ip pim join-filter iptv-channels out
```

Related Commands

ip access-list extended — configure an access list based on IP addresses or protocols.

ip pim ingress-interface-map

When the Dell Networking system is the RP, statically map potential incoming interfaces to (*,G) entries to create a lossless multicast forwarding environment.

Syntax

`ip pim ingress-interface-map` *`std-access-list`*

Parameters

std-access-list	Enter the name of a standard access list.

Defaults

none

Command Modes

INTERFACE

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell(conf)# ip access-list standard map1
Dell(config-std-nacl)# permit 224.0.0.1/24
Dell(config-std-nacl)#exit
Dell(conf)#int gig 1/1
Dell(config-if-gi-1/1)# ip pim ingress-interface-map map1
```

ip pim neighbor-filter

To prevent a router from participating in protocol independent multicast (PIM), configure this feature.

Syntax `ip pim neighbor-filter {access-list}`

To remove the restriction, use the `no ip pim neighbor-filter {access-list}` command.

Parameters

access-list	Enter the name of a standard access list. Maximum 16 characters.

Defaults none

Command Modes CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information Do not enter this command before creating the access-list.

ip pim query-interval

Change the frequency of PIM Router-Query messages.

Syntax `ip pim query-interval seconds`

To return to the default value, use the `no ip pim query-interval seconds` command.

Parameters

seconds	Enter a number as the number of seconds between router query messages. The range is from 0 to 65535. The default is **30 seconds**.

Defaults **30 seconds**

Command Modes INTERFACE

Command History	Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

ip pim register-filter

To prevent a PIM source DR from sending register packets to an RP for the specified multicast source and group, use this feature.

Syntax

`ip pim register-filter access-list`

To return to the default, use the `no ip pim register-filter access-list` command.

Parameters

access-list	Enter the name of an extended access list. Maximum 16 characters.

Defaults Not configured.

Command Modes CONFIGURATION

Command History	Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information The access name is an extended IP access list that denies PIM register packets to RP at the source DR based on the multicast and group addresses. Do not enter this command before creating the access-list.

ip pim rp-address

Configure a static PIM rendezvous point (RP) address for a group or access-list.

Syntax

`ip pim rp-address address {group-address group-address mask} override`

To remove an RP address, use the `no ip pim rp-address address {group-address group-address mask} override` command.

Parameters

address	Enter the RP address in dotted decimal format (A.B.C.D).
group-address *group-address mask*	Enter the keywords `group-address` then a group-address mask, in dotted decimal format (/xx), to assign that group address to the RP.
override	Enter the keyword `override` to override the BSR updates with static RP. The override takes effect immediately during enable/disable.

NOTE: This option is applicable to multicast group range.

Defaults	Not configured.
Command Modes	CONFIGURATION
Command History	Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	First-hop routers use this address by to send register packets on behalf of source multicast hosts. The RP addresses are stored in the order in which they are entered. RP addresses learned using BSR take priority over static RP addresses. Without the `override` option, RPs advertised by the BSR updates take precedence over the statically configured RPs.

ip pim rp-candidate

To send out a Candidate-RP-Advertisement message to the bootstrap (BS) router or define group prefixes that are defined with the RP address to PIM BSR, configure a PIM router.

Syntax

```
ip pim rp-candidate {interface [priority]
```

To return to the default value, use the `no ip pim rp-candidate {interface [priority]` command.

Parameters

interface	Enter the following keywords and slot/port or number information: • For a Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the slot/port information. • For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383. • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.
priority	(OPTIONAL) Enter the priority used in Bootstrap election process. The range is zero (0) to 255. The default is **192**.

Defaults	Not configured.
Command Modes	CONFIGURATION

Command History	Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Priority is stored at BSR router when receiving a Candidate-RP-Advertisement.

ip pim sparse-mode

Enable PIM sparse mode and IGMP on the interface.

Syntax

`ip pim sparse-mode`

To disable PIM sparse mode and IGMP, use the `no ip pim sparse-mode` command.

Defaults

Disabled.

Command Modes

INTERFACE

Command History	Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The interface must be enabled (the `no shutdown` command) and not have the `switchport` command configured. Multicast must also be enabled globally (using the `ip multicast-lag-hashing` command). PIM is supported on the port-channel interface.

ip pim sparse-mode sg-expiry-timer

Enable expiry timers globally for all sources, or for a specific set of (S,G) pairs an access list defines.

Syntax

`ip pim sparse-mode sg-expiry-timer` *`seconds`* `[access-list name]`

To disable configured timers and return to default mode, use the `no ip pim sparse-mode sg-expiry-timer` command.

Parameters

seconds	Enter the number of seconds the S, G entries are retained. The range is from 211 to 86400.
access-list name	(OPTIONAL) Enter the name of a previously configured Extended ACL to enable the expiry time to specified S,G entries.

Defaults

Disabled. The default expiry timer (with no times configured) is 210 sec.

Command Modes	CONFIGURATION
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	This command configures an expiration timer for all S.G entries, unless they are assigned to an Extended ACL.

ip pim spt-threshold

To switch to the shortest path tree when the traffic reaches the specified threshold value, configure the PIM router.

Syntax

`ip pim spt-threshold value | infinity`

To return to the default value, use the `no ip pim spt-threshold` command.

Parameters

value	(OPTIONAL) Enter the traffic value in kilobits per second. The default is **10 packets per second**. A value of zero (0) causes a switchover on the first packet.
infinity	(OPTIONAL) Enter the keyword `infinity` to never switch to the source-tree.

Defaults	Not configured.
Command Modes	CONFIGURATION
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	This command is applicable to last hop routers on the shared tree towards the rendezvous point (RP).

no ip pim snooping dr-flood

Disable the flooding of multicast packets to the PIM designated router.

Syntax

`no ip pim snooping dr-flood`

To re-enable the flooding of multicast packets to the PIM designated router, use the `ip pim snooping dr-flood` command.

Defaults	Enabled.

Command Modes	CONFIGURATION
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	By default, when you enable PIM-SM snooping, a switch floods all multicast traffic to the PIM designated router (DR), including unnecessary multicast packets. To minimize the traffic sent over the network to the designated router, you can disable `designated-router flooding`. When designated-router flooding is disabled, PIM-SM snooping only forwards the multicast traffic, which belongs to a multicast group for which the switch receives a join request, on the port connected towards the designated router. If the PIM DR flood is not disabled (default setting): • Multicast traffic is transmitted on the egress port towards the PIM DR if the port is not the incoming interface. • Multicast traffic for an unknown group is sent on the port towards the PIM DR. When DR flooding is disabled, multicast traffic for an unknown group is dropped.
Related Commands	ip pim sparse-mode — enables PIM-SM snooping.

show ip pim bsr-router

View information on the Bootstrap router.

Syntax

`show ip pim bsr-router`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
E600-7-rpm0#show ip pim bsr-router
PIMv2 Bootstrap information
This system is the Bootstrap Router (v2)
  BSR address: 7.7.7.7 (?)
  Uptime: 16:59:06, BSR Priority: 0, Hash mask length: 30
  Next bootstrap message in 00:00:08

This system is a candidate BSR
  Candidate BSR address: 7.7.7.7, priority: 0, hash mask
length: 30
```

show ip pim interface

View information on the interfaces with IP PIM enabled.

Syntax `show ip pim interface`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show ip pim interface` command shown in the following example.

Field	Description
Address	Lists the IP addresses of the interfaces participating in PIM.
Interface	List the interface type, with either slot/port information or ID (VLAN or Port Channel), of the interfaces participating in PIM.
Ver/Mode	Displays the PIM version number and mode for each interface participating in PIM: • v2 = PIM version 2 • S = PIM Sparse mode
Nbr Count	Displays the number of PIM neighbors discovered over this interface.
Query Intvl	Displays the query interval for Router Query messages on that interface (configured with `ip pim query-interval` command).
DR Prio	Displays the Designated Router priority value configured on the interface (use the `ip pim dr-priority` command).
DR	Displays the IP address of the Designated Router for that interface.

Example

```
E600-7-RPM0#show ip pim interface
Address         Interface Ver/ Nbr   Query DR   DR
                          Mode Count Intvl Prio
172.21.200.254 Gi 7/9    v2/S 0     30 1  172.21.200.254
172.60.1.2     Gi 7/11   v2/S 0     30 1  172.60.1.2
192.3.1.1      Gi 7/16   v2/S 1     30 1  192.3.1.1
192.4.1.1      Gi 13/5   v2/S 0     30 1  192.4.1.1
172.21.110.1   Gi 13/6   v2/S 0     30 1  172.21.110.1
172.21.203.1   Gi 13/7   v2/S 0     30 1  172.21.203.1
```

show ip pim neighbor

View PIM neighbors.

Syntax	`show ip pim neighbor`
Command Modes	- EXEC - EXEC Privilege
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	The following describes the `show ip pim neighbor` command shown in the following example.

Field	Description
Neighbor address	Displays the IP address of the PIM neighbor.
Interface	List the interface type, with either slot/port information or ID (VLAN or Port Channel), on which the PIM neighbor was found.
Uptime/expires	Displays the amount of time the neighbor has been up then the amount of time until the neighbor is removed from the multicast routing table (that is, until the neighbor hold time expires).
Ver	Displays the PIM version number. • v2 = PIM version 2
DR prio/Mode	Displays the Designated Router priority and the mode. • 1 = default Designated Router priority (use the `ip pim dr-priority` command) • DR = Designated Router • S = Sparse mode

Example

```
Dell#show ip pim neighbor
Neighbor   Interface  Uptime/Expires    Ver   DR
Address                                       Prio/Mode
127.87.3.4 Gi 7/16    09:44:58/00:01:24  v2   1 / S
Dell#
```

show ip pim rp

View all multicast groups-to-RP mappings.

Syntax `show ip pim rp [mapping | group-address]`

Parameters

mapping	(OPTIONAL) Enter the keyword `mapping` to display the multicast groups-to-RP mapping and information on how RP is learnt.
group-address	(OPTIONAL) Enter the multicast group address mask in dotted decimal format to view RP for a specific group.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#sh ip pim rp
Group           RP
224.2.197.115   165.87.20.4
224.2.217.146   165.87.20.4
224.3.3.3       165.87.20.4
225.1.2.1       165.87.20.4
225.1.2.2       165.87.20.4
229.1.2.1       165.87.20.4
229.1.2.2       165.87.20.4
Dell#
```

Example (Mapping)

```
Dell#sh ip pim rp mapping
Group(s): 224.0.0.0/4
  RP: 165.87.20.4, v2
    Info source: 165.87.20.5, via bootstrap, priority 0
      Uptime: 00:03:11, expires: 00:02:46
  RP: 165.87.20.3, v2
    Info source: 165.87.20.5, via bootstrap, priority 0
      Uptime: 00:03:11, expires: 00:03:03

Dell#
```

Example (Address)

```
Dell#sh ip pim rp 229.1.2.1
Group         RP
229.1.2.1    165.87.20.4

Dell#
```

show ip pim snooping interface

Display information on VLAN interfaces with PIM-SM snooping enabled.

Syntax `show ip pim snooping interface [vlan vlan-id]`

Parameters

vlan *vlan-id*	(OPTIONAL) Enter a VLAN ID to display information about a specified VLAN configured for PIM-SM snooping. The valid VLAN IDs range is from 1 to 4094.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show ip pim snooping interface` commands shown in the following example.

Field	Description
Interface	Displays the VLAN interfaces with PIM-SM snooping enabled.
Ver/Mode	Displays the PIM version number for each VLAN interface with PIM-SM snooping enabled: • v2 = PIM version 2 • S = PIM Sparse mode
Nbr Count	Displays the number of neighbors learned through PIM-SM snooping on the interface.
DR Prio	Displays the Designated Router priority value configured on the interface (`ip pim dr-priority` command).
DR	Displays the IP address of the Designated Router for that interface.

Example (#2)

```
Dell#show ip pim snooping interface
Interface Ver Nbr    DR    DR
              Count  Prio
Vlan 2    v2  3      1     165.87.32.2
```

show ip pim snooping neighbor

Display information on PIM neighbors learned through PIM-SM snooping.

Syntax

```
show ip pim snooping neighbor [vlan vlan-id]
```

Parameters

vlan *vlan-id*	(OPTIONAL) Enter a VLAN ID to display information about PIM neighbors that PIM-SM snooping discovered on a specified VLAN. The valid VLAN IDs range is from 1 to 4094.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show ip pim snooping neighbor` commands shown in the following example.

Field	Description
Neighbor address	Displays the IP address of the neighbor learned through PIM-SM snooping.
Interface	Displays the VLAN ID number and slot/port on which the PIM-SM-enabled neighbor was discovered.
Uptime/expires	Displays the amount of time the neighbor has been up then the amount of time until the neighbor is removed from the multicast routing table (that is, until the neighbor hold time expires).
Ver	Displays the PIM version number: • v2 = PIM version 2
DR prio/Mode	Displays the Designated Router priority and the mode: • 1 = default Designated Router priority (use the `ip pim dr-priority` command) • DR = Designated Router • S = Sparse mode

Example

```
Dell#show ip pim snooping neighbor

Neighbor    Interface          Uptime/Expires    Ver  DR Prio
Address
165.87.32.2   Vl 2 [Gi 4/13 ]  00:04:03/00:01:42  v2  1
165.87.32.10  Vl 2 [Gi 4/11 ]  00:00:46/00:01:29  v2  0
165.87.32.12  Vl 2 [Gi 4/20 ]  00:00:51/00:01:24  v2  0
```

show ip pim snooping tib

Display information from the tree information base (TIB) PIM-SM snooping discovered about multicast group members and states.

Syntax `show ip pim snooping tib [vlan *vlan-id*] [*group-address* [*source-address*]]`

Parameters

vlan *vlan-id*	(OPTIONAL) Enter a VLAN ID to display TIB information PIM-SM snooping discovered on a specified VLAN. The valid VLAN IDs range is from 1 to 4094.

group-address	(OPTIONAL) Enter the group address in dotted decimal format (A.B.C.D) to display TIB information PIM-SM snooping discovered for a specified multicast group.
source-address	(OPTIONAL) Enter the source address in dotted decimal format (A.B.C.D) to display TIB information PIM-SM snooping discovered for a specified multicast source.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show ip pim snooping tib` commands shown in the following example.

Field	Description
(S, G)	Displays the entry in the PIM multicast snooping database.
uptime	Displays the amount of time the entry has been in the PIM multicast route table.
expires	Displays the amount of time until the entry expires and is removed from the database.
RP	Displays the IP address of the RP/source for this entry.
flags	List the flags to define the entries: • S = PIM Sparse Mode • C = directly connected • L = local to the multicast group • P = route was pruned • R = the forwarding entry is pointing toward the RP • F = Dell Networking OS is registering this entry for a multicast source • T = packets were received via Shortest Tree Path • J = first packet from the last hop router is received and the entry is ready to switch to SPT • K=acknowledge pending state
Incoming interface	Displays the reverse path forwarding (RPF) interface towards the RP/ source.
RPF neighbor	Displays the next hop from this interface towards the RP/ source.
Outgoing interface list:	Lists the interfaces that meet one of the following criteria: • a directly connect member of the Group • statically configured member of the Group

Field	Description
	- received a (*,G) Join message

Example

```
Dell#show ip pim snooping tib

PIM Multicast Snooping Table
Flags: J/P - (*,G) Join/Prune, j/p - (S,G) Join/Prune
       SGR-P - (S,G,R) Prune
Timers: Uptime/Expires
* : Inherited port

(*, 225.1.2.1), uptime 00:00:01, expires 00:02:59, RP
165.87.70.1, flags: J
  Incoming interface: Vlan 2, RPF neighbor 0.0.0.0
  Outgoing interface list:
    GigabitEthernet 4/11 RPF 165.87.32.2 00:00:01/00:02:59
    GigabitEthernet 4/13 Upstream Port   -/-

Dell#show ip pim snooping tib vlan 2 225.1.2.1 165.87.1.7

PIM Multicast Snooping Table
Flags: J/P - (*,G) Join/Prune, j/p - (S,G) Join/Prune
       SGR-P - (S,G,R) Prune
Timers: Uptime/Expires
* : Inherited port

(165.87.1.7, 225.1.2.1), uptime 00:00:08, expires 00:02:52,
flags: j
  Incoming interface: Vlan 2, RPF neighbor 0.0.0.0
  Outgoing interface list:
    GigabitEthernet 4/11 Upstream Port    -/-
    GigabitEthernet 4/13 DR Port          -/-
    GigabitEthernet 4/20 RPF 165.87.32.10 00:00:08/00:02:52
```

show ip pim summary

View information about PIM-SM operation.

Syntax `show ip pim summary`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show ip pim summary

PIM TIB version 495
Uptime 22:44:52
Entries in PIM-TIB/MFC : 2/2

Active Modes :
        PIM-SNOOPING
```

```
Interface summary:
        1 active PIM interface
        0 passive PIM interfaces
        3 active PIM neighbors

TIB summary:
       1/1 (*,G) entries in PIM-TIB/MFC
       1/1 (S,G) entries in PIM-TIB/MFC
       0/0 (S,G,Rpt) entries in PIM-TIB/MFC

       0 PIM nexthops
       0 RPs
       0 sources
       0 Register states

Message summary:
       2582/2583 Joins sent/received
       5/0 Prunes sent/received
       0/0 Candidate-RP advertisements sent/received
       0/0 BSR messages sent/received
       0/0 State-Refresh messages sent/received
       0/0 MSDP updates sent/received
       0/0 Null Register messages sent/received
       0/0 Register-stop messages sent/received

Data path event summary:
       0 no-cache messages received
       0 last-hop switchover messages received
       0/0 pim-assert messages sent/received
       0/0 register messages sent/received

Memory usage:
       TIB             : 3768 bytes
       Nexthop cache   : 0 bytes
       Interface table : 992 bytes
       Neighbor table  : 528 bytes
       RP Mapping      : 0 bytes
```

show ip pim tib

View the PIM tree information base (TIB).

Syntax `show ip pim tib [`*`group-address`*` [`*`source-address`*`]]`

Parameters

group-address	(OPTIONAL) Enter the group address in dotted decimal format (A.B.C.D).
source-address	(OPTIONAL) Enter the source address in dotted decimal format (A.B.C.D).

Command Modes

- EXEC
- EXEC Privilege

Command History	Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show ip pim tib` command shown in the following example.

Field	Description
(S, G)	Displays the entry in the multicast PIM database.
uptime	Displays the amount of time the entry has been in the PIM route table.
expires	Displays the amount of time until the entry expires and is removed from the database.
RP	Displays the IP address of the RP/source for this entry.
flags	List the flags to define the entries: • D = PIM Dense Mode • S = PIM Sparse Mode • C = directly connected • L = local to the multicast group • P = route was pruned • R = the forwarding entry is pointing toward the RP • F = Dell Networking OS is registering this entry for a multicast source • T = packets were received via Shortest Tree Path • J = first packet from the last hop router is received and the entry is ready to switch to SPT • K = acknowledge pending state
Incoming interface	Displays the reverse path forwarding (RPF) interface towards the RP/ source.
RPF neighbor	Displays the next hop from this interface towards the RP/ source.
Outgoing interface list:	Lists the interfaces that meet one of the following criteria: • a directly connect member of the Group • statically configured member of the Group • received a (*,G) Join message

Example

```
Dell#show ip pim tib

PIM Multicast Routing Table
Flags:D- Dense, S- Sparse, C- Connected, L- Local, P- Pruned,
      R- RP-bit set, F- Register flag, T- SPT-bit set, J- Join
SPT,
      M- MSDP created entry, A- Candidate for MSDP
Advertisement,
      K- Ack-Pending State
Timers: Uptime/Expires
```

```
Interface state: Interface, next-Hop, State/Mode

(*, 226.1.1.1), uptime 01:29:19, expires 00:00:52, RP
10.211.2.1, flags: SCJ
  Incoming interface: GigabitEthernet 4/23, RPF neighbor
10.211.1.2
  Outgoing interface list:
    GigabitEthernet 8/0

(*, 226.1.1.2), uptime 00:18:08, expires 00:00:52, RP
10.211.2.1, flags: SCJ
  Incoming interface: GigabitEthernet 4/23, RPF neighbor
10.211.1.2
  Outgoing interface list:
    GigabitEthernet 8/0

(*, 226.1.1.3), uptime 00:18:08, expires 00:00:52, RP
10.211.2.1, flags: SCJ
  Incoming interface: GigabitEthernet 4/23, RPF neighbor
10.211.1.2
  Outgoing interface list:
    GigabitEthernet 8/0

(*, 226.1.1.4), uptime 00:18:08, expires 00:00:52, RP
10.211.2.1, flags: SCJ
  Incoming interface: GigabitEthernet 4/23, RPF neighbor
10.211.1.2
  Outgoing interface list:
    GigabitEthernet 8/0
```

show running-config pim

Display the current configuration of PIM-SM snooping.

Syntax `show running-config pim`

Command Modes EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show running-config pim
!
ip pim snooping enable
```

Related Commands ip pim sparse-mode — enables PIM-SM snooping.

IPv6 PIM-Sparse Mode Commands

The following describes the IPv6 PIM-sparse mode (PIM-SM) commands.

ipv6 pim bsr-border

Define the border of PIM domain by filtering inbound and outbound PIM-BSR messages per interface.

Syntax	`ipv6 pim bsr-border`
Defaults	Disabled.
Command Modes	INTERFACE
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	This command is applied to the subsequent PIM-BSR messages. Existing BSR advertisements are cleaned up by time-out.

ipv6 pim bsr-candidate

Configure the router as a bootstrap (BSR) candidate.

Syntax

```
ipv6 pim bsr-candidate interface [hash-mask-length] [priority]
```

To disable the bootstrap candidate, use the `no ipv6 pim bsr-candidate` command.

Parameters

interface	Enter the following keywords and slot/port or number information: • For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383. • For a Port Channel interface, enter the keywords `port-channel` then a number. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.
hash-mask-length	(OPTIONAL) Enter the hash mask length for RP selection. The range is from 0 to 128. The default is **126**.
priority	(OPTIONAL) Enter the priority value for Bootstrap election process. The range is from 0 to 255. The default is **0**.

Defaults	Refer to Parameters.
Command Modes	CONFIGURATION
Command History	Version 9.2(0.0) — Introduced on the MXL 10/40GbE Switch IO Module.

ipv6 pim dr-priority

Change the designated router (DR) priority for the IPv6 interface.

Syntax

`ipv6 pim dr-priority` *`priority-value`*

To remove the DR priority value assigned, use the `no ipv6 pim dr-priority` command.

Parameters

priority-value	Enter a number. Preference is given to larger/higher number. The range is from 0 to 4294967294. The default is **1**.

Defaults	**1**
Command Modes	INTERFACE
Command History	Version 9.2(0.0) — Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	The router with the largest value assigned to an interface becomes the designated router. If two interfaces contain the same designated router priority value, the interface with the largest interface IP address becomes the designated router.

ipv6 pim join-filter

Permit or deny PIM Join/Prune messages on an interface using an access list. This command prevents the PIM-SM router from creating state based on multicast source and/or group.

Syntax

`ipv6 pim join-filter` *`access-list`*

Parameters

access-list	Enter the name of an extended access list.
in	Enter the keyword `in` to apply the access list to inbound traffic.
out	Enter the keyword `out` to apply the access list to outbound traffic.

Defaults	none
Command Modes	INTERFACE
Command History	Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell(conf)#ipv6 access-list JOIN-FIL_ACL
Dell(conf-ipv6-acl)#permit ipv6 165:87:34::0/112 ff0e::
225:1:2:0/112
Dell(conf-ipv6-acl)#permit ipv6 any ff0e::230:1:2:0/112
Dell(conf-ipv6-acl)#permit ipv6 165:87:32::0/112 any
Dell(conf-ipv6-acl)#exit
Dell(conf)#interface gigabitethernet 0/84
Dell(conf-if-gi-0/84)#ipv6 pim join-filter JOIN-FIL_ACL in
Dell(conf-if-gi-0/84)#ipv6 pim join-filter JOIN-FIL_ACL out
```

ipv6 pim query-interval

Change the frequency of IPv6 PIM router-query messages.

Syntax

```
ipv6 pim query-interval seconds
```

To return to the default value, use the `no ipv6 pim query-interval seconds` command.

Parameters

seconds	Enter a number as the number of seconds between router query messages. The range is from 0 to 65535. The default is **30 seconds**.

Defaults	**30 seconds**
Command Modes	INTERFACE
Command History	Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

ipv6 pim neighbor-filter

Prevent the system from forming a PIM adjacency with a neighboring system.

Syntax

```
ipv6 pim neighbor-filter {access-list}
```

Parameters

access-list	Enter the name of a standard access list. Maximum 16 characters.

Defaults	none
Command Modes	CONFIGURATION
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	Do not enter this command before creating the access-list.

ipv6 pim register-filter

Configure the source DR so that it does not send register packets to the RP for the specified sources and groups.

Syntax `ipv6 pim register-filter` *`access-list`*

Parameters

access-list	Enter the name of the extended ACL that contains the sources and groups to filter.

Defaults	none
Command Modes	CONFIGURATION
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell(conf)#ipv6 pim register-filter REG-FIL_ACL
Dell(conf)#ipv6 access-list REG-FIL_ACL
Dell(conf-ipv6-acl)#deny ipv6 165:87:34::10/128 ff0e::
225:1:2:0/112
Dell(conf-ipv6-acl)#permit ipv6 any any
Dell(conf-ipv6-acl)#exit
```

ipv6 pim rp-address

Configure a static PIM rendezvous point (RP) address for a group. First-hop routers use this address to send register packets on behalf of the source multicast host.

Syntax `ipv6 pim rp-address` *`address`* `group-address` *`group-address mask`* `override`

To remove an RP address, use the `no ipv6 pim re-address` *`address`* `group-address` *`mask`* `override` command.

Parameters

address	Enter the IPv6 RP address in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zero.
group-address *group-address mask*	Enter the keywords `group-address` then the group address in the x:x:x:x::x format and then the mask in /nn format to assign that group address to the RP. **NOTE:** The :: notation specifies successive hexadecimal fields of zero.
override	Enter the keyword `override` to override the BSR updates with static RP. The override takes effect immediately during enable/disable. **NOTE:** This option is applicable to multicast group range.

Defaults none

Command Modes CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The RP addresses are stored in the order in which they are entered. RP addresses learned via BSR take priority over static RP addresses.

Without the override option, the BSR-advertised RPs updates take precedence over the statically configured RPs.

ipv6 pim rp-candidate

Specify an interface as an RP candidate.

Syntax

```
ipv6 pim rp-candidate interface [priority-value]
```

Parameters

interface	Enter the following keywords and slot/port or number information: • For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383. • For a Port Channel interface, enter the keywords `port-channel` then a number. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

priority-value	(OPTIONAL) Enter a number as the priority of this RP Candidate, which is included in the Candidate-RP-Advertisements. The range is 0 (highest) to 255 (lowest).

Defaults none

Command Modes CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

ipv6 pim sparse-mode

Enable IPv6 PIM sparse mode on the interface.

Syntax `ipv6 pim sparse-mode`

To disable IPv6 PIM sparse mode, use the `no ipv6 pim sparse-mode` command.

Defaults Disabled.

Command Modes INTERFACE

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information Enable the interface (use the `no shutdown` command) and not have the `switchport` command configured. Also enable Multicast globally. PIM is supported on the port-channel interface.

ipv6 pim spt-threshold

Specifies when a PIM leaf router should join the shortest path tree.

Syntax `ipv6 pim spt-threshold {kbps | infinity}`

To return to the default value, use the `no ipv6 pim spt-threshold` command.

Parameters

kbps	Enter a traffic rate in kilobytes per second. The range is from 0 to 4294967 kbps. The default is **10 kbps**.
infinity	Enter the keyword `infinity` to have all sources for the specified group use the shared tree and never join shortest path tree (SPT).

Defaults	**10 kbps**
Command Modes	CONFIGURATION
Command History	Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	PIM leaf routers join the shortest path tree immediately after the first packet arrives from a new source.

show ipv6 pim bsr-router

View information on the Bootstrap router (v2).

Syntax `show ipv6 pim bsr-router`

Command Modes

- EXEC
- EXEC Privilege

Command History Version 9.2(0.0)

Example

```
Dell#show ipv6 pim bsr-router
PIMv2 Bootstrap information
This system is the Bootstrap Router (v2)
  BSR address: 14::2
  Uptime:      00:02:54, BSR Priority: 0, Hash mask length: 126
  Next bootstrap message in 00:00:06

This system is a candidate BSR
  Candidate BSR address: 14::2, priority: 0, hash mask length:
126
Dell
```

show ipv6 pim interface

Display IPv6 PIM enabled interfaces.

Syntax `show ipv6 pim interface`

Command Modes

- EXEC
- EXEC Privilege

Command History	Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show ipv6 pim interface
Interface Ver/ Nbr   Query DR
          Mode Count Intvl Prio

Gi 10/3   v2/S 1     30    1
  Address : fe80::201:e8ff:fe02:140f
  DR : this router

Gi 10/11  v2/S 0     30    1
  Address : fe80::201:e8ff:fe02:1417
  DR : this router
Dell#
```

show ipv6 pim neighbor

Displays IPv6 PIM neighbor information.

Syntax `show ipv6 pim neighbor [detail]`

Parameters

detail	(OPTIONAL) Enter the keyword `detail` to displayed PIM neighbor detailed information.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show ipv6 pim neighbor detail
Neighbor Interface Uptime/Expires Ver DR
Address                                Prio/Mode
fe80::201:e8ff:fe00:6265 Gi 10/3 00:07:39/00:01:42 v2 1 / S
165:87:50::6
Dell#
```

show ipv6 pim rp

View all multicast groups-to-RP mappings.

Syntax `show ipv6 pim rp [mapping | group-address]`

Parameters

mapping	(OPTIONAL) Enter the keyword `mapping` to display the multicast groups-to-RP mapping and information on how RP is learnt.
group-address	(OPTIONAL) Enter the multicast group address mask in dotted decimal format to view RP for a specific group.

Command Modes	- EXEC - EXEC Privilege

Command History	**Version 9.2(0.0)**	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dellshow ipv6 pim rp
Group RP
ff0e::225:1:2:1 14::1
ff0e::225:1:2:2 14::1
ff0e::226:1:2:1 14::1
ff0e::226:1:2:2 14::1
Dell
```

Example (Mapping)

```
Dellshow ipv6 pim rp mapping
PIM Group-to-RP Mappings
Group(s): ff00::/8
  RP: 14::1, v2
    Info source: 14::1, via bootstrap, priority 192
       Uptime: 00:03:37, expires: 00:01:53
Group(s): ff00::/8, Static
  RP: 14::2, v2
Dell
```

show ipv6 pim tib

View the IPv6 PIM multicast-routing database (tree information base — tib).

Syntax `show ipv6 pim tib [group-address [source-address]]`

Parameters

group-address	(OPTIONAL) Enter the multicast group address in the x:x:x:x::x format to view RP mappings for a specific group. **NOTE:** The :: notation specifies successive hexadecimal fields of zero.
source-address	(OPTIONAL) Enter the source address in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zero.

Command Modes	- EXEC - EXEC Privilege

Command History	**Version 9.2(0.0)**	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show ipv6 pim tib
```

```
PIM Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L - Local, P -
Pruned,
       R - RP-bit set, F - Register flag, T - SPT-bit set, J -
Join SPT,
       M - MSDP created entry, A - Candidate for MSDP
Advertisement
       K - Ack-Pending State
Timers: Uptime/Expires
Interface state: Interface, next-Hop, State/Mode

(25::1, ff0e::225:1:2:1), uptime 00:09:53, expires
00:00:00,flags: CJ
  RPF neighbor: GigabitEthernet 10/3, fe80::201:e8ff:fe00:6265
  Outgoing interface list:
    GigabitEthernet 10/11

(25::1, ff0e::225:1:2:2), uptime 00:09:54, expires
00:00:00,flags: CJ
  RPF neighbor: GigabitEthernet 10/3, fe80::201:e8ff:fe00:6265
  Outgoing interface list:
    GigabitEthernet 10/11

(25::2, ff0e::225:1:2:2), uptime 00:09:54, expires
00:00:00,flags: CJ
  RPF neighbor: GigabitEthernet 10/3, fe80::201:e8ff:fe00:6265
  Outgoing interface list:
    GigabitEthernet 10/11

(25::1, ff0e::226:1:2:1), uptime 00:09:54, expires
00:00:00,flags: CJ
  RPF neighbor: GigabitEthernet 10/3, fe80::201:e8ff:fe00:6265
  Outgoing interface list:
    GigabitEthernet 10/11
Dell#
```

40

Port Monitoring

The port monitoring feature allows you to monitor network traffic by forwarding a copy of each incoming or outgoing packet from one port to another port.

Important Points to Remember

- Port monitoring is supported on physical ports and logical interfaces, such as Port Channels and virtual local area networks (VLANs).
- The monitoring (destination, "MG") and monitored (source, "MD") ports must be on the same switch.
- In general, a monitoring port should have `no ip address` and `no shutdown` as the only configuration; Dell Networking operating software permits a limited set of commands for monitoring ports; display them using the `?` command. A monitoring port also may not be a member of a VLAN.
- A total of 4 MG can be configured in a single port-pipe.
- MG and MD ports can reside anywhere across a port-pipe.
- Dell Networking operating software supports multiple source ports to be monitored by a single destination port in one monitor session.
- One monitor session can have only one MG port.

NOTE: The monitoring port should not be a part of any other configuration.

Description

Enter a description of this monitoring session.

Syntax `description {`*`description`*`}`

To remove the description, use the `no description {`*`description`*`}` command.

Parameters

description	Enter a description regarding this session (80 characters maximum).

Defaults none

Command Modes CONFIGURATION

Command History

Version 9.4(0.0)	Added support for the RPM / ERPM.

Version 8.3.16.1	Introduced on the M I/O Aggregator.

Related Commands monitor session — enables a monitoring session.

flow-based enable

Enable flow-based monitoring.

Syntax

```
flow-based enable
```

To disable flow-based monitoring, use the `no flow-based enable` command.

Defaults Disabled, that is flow-based monitoring is not applied.

Command Modes MONITOR SESSION (conf-mon-*sess-session-ID*)

Command History

Version 9.4(0.0)	Added support for the RPM/ERPM.
Version 9.3(0.0)	Introduced on the MXL 10/40GbE Switch IO Module platform.
Version 8.1.1.0	Introduced on the E-Series ExaScale.
Version 7.4.1.0	Introduced on the E-Series.

Usage Information To monitor traffic with particular flows the interface, appropriate ACLs has be applied in ingress direction. Flow- based is not supported in the tx direction. Even though we can configure it in both the direction, only rx will work.

The flow- based enable command has to be applied as a **monitor session** with some configuration which is already present in it, other wise flow- based will not take effect.

Related Commands monitor session – enables a monitoring session.

monitor session

Create a session for monitoring traffic with port monitoring.

Syntax

```
monitor session session-ID (type { rpm | erpm })
```

To delete a session, use the `no monitor session session-ID` command.

To delete all monitor sessions, use the `no monitor session all` command.

Parameters

session-ID	Enter a session identification number. The range is from 0 to 65535.
type *rpm* | *erpm*	Specifies one of the following type: • rpm: to create remote port monitoring session. • erpm: to create encapsulated remote port monitoring session. • If no option is specified, by default SPAN will be created.

Defaults none

Command Modes CONFIGURATION

Command History

Version 9.4(0.0)	Added support for rpm / erpm.
Version 8.3.16.1	Introduced on the M I/O Aggregator.

Usage Information The `monitor` command is saved in the running configuration at Monitor Session mode level and can be restored after a chassis reload.

Example

```
Dell(conf)# monitor session 60
Dell(conf-mon-sess-60)
```

Related Command

show monitor session — displays the monitor session.

show running-config monitor session — displays the running configuration of a monitor session.

show config

Display the current monitor session configuration.

Syntax `show config`

Defaults none

Command Modes MONITOR SESSION (conf-mon-*sess-session-ID*)

Command History

Version 8.3.16.1	Introduced on the M I/O Aggregator.

Example

```
Dell(conf-mon-sess-1)#show config
!
monitor session 1
 source TenGigabitEthernet 0/1 destination Port-channel 1
direction rx
```

show monitor session

Display the monitor information of a particular session or all sessions.

Syntax

`show monitor session {session-ID}`

To display monitoring information for all sessions, use the `show monitor session` command.

Parameters

session-ID	(OPTIONAL) Enter a session identification number. The range is from 0 to 65535.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.4.0.0	Added support for the RPM / ERPM.
Version 8.3.16.1	Introduced on the M I/O Aggregator.

Example

```
Dell#show monitor session
  SessID  Source         Destination        Dir  Mode  Source
IP      Dest IP
  ------  ------         -----------        ---  ----
---------      --------
     1   Vl 10             Te 0/8           rx   Flow     N/
A            N/A
```

Related Commands

monitor session — creates a session for monitoring.

show running-config monitor session

Display the running configuration of all monitor sessions or a specific session.

Syntax

`show running-config monitor session {session-ID}`

To display the running configuration for all monitor sessions, use the `show running-config monitor session` command.

Parameters

session-ID	(OPTIONAL) Enter a session identification number. The range from 0 to 65535.

Defaults

none

Command Modes

- EXEC

- EXEC Privilege

Command History		
	Version 8.3.16.1	Introduced on the M I/O Aggregator.

Usage Information

The `monitoring` command is saved in the running configuration at the Monitor Session mode level and can be restored after a chassis reload.

Example

```
Dell# show running-config monitor session
!
monitor session 1
source TenGigabitEthernet 0/1 destination TenGigabitEthernet
0/2 direction rx
```

Related Commands

monitor session — creates a session for monitoring.

show monitor session — displays a monitor session.

source (port monitoring)

Configure a port monitor source.

Syntax

`source interface | range destination interface direction {rx | tx | both}`

To disable a monitor source, use the `no source interface destination interface direction {rx | tx | both}` command.

Parameters

source *interface*	Enter the one of the following keywords and slot/port information: • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a VLAN interface enter the keyword `VLAN` then by a number range from 1 to 4094. • For a port channel interface, enter the keyword `LAG` then port channel and the port-channel id .
range	Enter the keyword `range` to specify a list of interfaces.
destination	Enter the keyword `destination` to specify the destination interface. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

	- For a port channel interface, enter the keyword `LAG` then port channel and the port-channel id .
interface	Enter the one of the following keywords and slot/port information: - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. - For a VLAN interface enter the keyword `VLAN` followed by a number from 1 to 4094. - For a port channel interface, enter the keyword `LAG` then port channel and the port-channel id .
direction {rx | tx | both}	Enter the keyword `direction` then one of the packet directional indicators. - `rx`: to monitor receiving packets only. - `tx`: to monitor transmitting packets only. - `both`: to monitor both transmitting and receiving packets.

Defaults none

Command Modes MONITOR SESSION (conf-mon-*sess-session-ID*)

Command History

Version 9.4(0.0)	Added support for Source and destination.
Version 8.3.16.1	Introduced on the M I/O Aggregator.

Example

```
Dell# monitor session 0
source Port-channel 10 destination TenGigabitEthernet 0/33
direction tx
```

41

Private VLAN (PVLAN)

Private VLANs extend the Dell Networking OS security suite by providing Layer 2 isolation between ports within the same private VLAN. A private VLAN partitions a traditional VLAN into subdomains identified by a primary and secondary VLAN pair.

The Dell Networking OS private VLAN implementation is based on RFC 3069.

For more information, refer to the following commands. The command output is augmented in the Dell Networking OS version 7.8.1.0 at later to provide PVLAN data:

- show arp
- show vlan

Private VLAN Concepts

Primary VLAN:

The primary VLAN is the base VLAN and can have multiple secondary VLANs. There are two types of secondary VLAN — community VLAN and isolated VLAN:

- A primary VLAN can have any number of community VLANs and isolated VLANs.
- Private VLANs block all traffic to isolated ports except traffic from promiscuous ports. Traffic received from an isolated port is forwarded only to promiscuous ports or trunk ports.

Community VLAN:

A community VLAN is a secondary VLAN of the primary VLAN:

- Ports in a community VLAN can talk to each other. Also, all ports in a community VLAN can talk to all promiscuous ports in the primary VLAN and vice versa.
- Devices on a community VLAN can communicate with each other using member ports, while devices in an isolated VLAN cannot.

Isolated VLAN:

An isolated VLAN is a secondary VLAN of the primary VLAN:

- Ports in an isolated VLAN cannot talk to each other. Servers would be mostly connected to isolated VLAN ports.
- Isolated ports can talk to promiscuous ports in the primary VLAN, and vice versa.

Port Types:

- *Community port*: A community port is a port that belongs to a community VLAN and is allowed to communicate with other ports in the same community VLAN and with promiscuous ports.

- *Isolated port*: An isolated port is a port that, in Layer 2, can only communicate with promiscuous ports that are in the same PVLAN.
- *Promiscuous port*: A promiscuous port is a port that is allowed to communicate with any other port type.
- *Trunk port*: A trunk port carries VLAN traffic across switches:
  - A trunk port in a PVLAN is always tagged.
  - A trunk port in Tagged mode carries primary or secondary VLAN traffic. The tag on the packet helps identify the VLAN to which the packet belongs.
  - A trunk port can also belong to a regular VLAN (non-private VLAN).

ip local-proxy-arp

Enable/disable Layer 3 communication between secondary VLANs in a private VLAN.

Syntax

`[no] ip local-proxy-arp`

To disable Layer 3 communication between secondary VLANs in a private VLAN, use the `no ip local-proxy-arp` command in INTERFACE VLAN mode for the primary VLAN.

To disable Layer 3 communication in a particular secondary VLAN, use the `no ip local-proxy-arp` command in INTERFACE VLAN mode for the selected secondary VLAN.

NOTE: Even after you disable `ip-local-proxy-arp` (use `no ip-local-proxy-arp`) in a secondary VLAN, Layer 3 communication may happen between some secondary VLAN hosts, until the address resolution protocol (ARP) timeout happens on those secondary VLAN hosts.

Defaults

Layer 3 communication is disabled between secondary VLANs in a private VLAN.

Command Modes

INTERFACE VLAN

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

private-vlan mode — sets the mode of the selected VLAN to community, isolated, or primary.

private-vlan mapping secondary-vlan — maps secondary VLANs to the selected primary VLAN.

show arp — displays the ARP table.

show interfaces private-vlan — displays the type and status of the PVLAN interfaces.

show vlan private-vlan — displays the PVLANs and/or interfaces that are part of a PVLAN.

switchport mode private-vlan — sets PVLAN mode of the selected port.

private-vlan mapping secondary-vlan

Map secondary VLANs to the selected primary VLAN.

Syntax	`[no] private-vlan mapping secondary-vlan vlan-list` To remove specific secondary VLANs from the configuration, use the `no private-vlan mapping secondary-vlan vlan-list` command syntax.

Parameters

vlan-list	Enter the list of secondary VLANs to associate with the selected primary VLAN. The list can be in comma-delimited or hyphenated-range format, following the convention for the range input.

Defaults	none
Command Modes	INTERFACE VLAN

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The list of secondary VLANs can be:

- Specified in comma-delimited or hyphenated-range format.
- Specified with this command even before they have been created.
- Amended by specifying the new secondary VLAN to be added to the list.

Related Commands

private-vlan mode — sets the mode of the selected VLAN to community, isolated, or primary.

show interfaces private-vlan — displays the type and status of the PVLAN interfaces.

show vlan private-vlan — displays the PVLANs and/or interfaces that are part of a PVLAN.

show vlan private-vlan mapping — displays the primary-secondary VLAN mapping.

switchport mode private-vlan — sets PVLAN mode of the selected port.

private-vlan mode

Set PVLAN mode of the selected VLAN to community, isolated, or primary.

Syntax

```
[no] private-vlan mode {community | isolated | primary}
```

To remove the PVLAN configuration, use the `no private-vlan mode {community | isolated | primary}` command syntax.

Parameters

community	Enter the keyword `community` to set the VLAN as a community VLAN.
isolated	Enter the keyword `isolated` to configure the VLAN as an isolated VLAN.
primary	Enter the keyword `primary` to configure the VLAN as a primary VLAN.

Defaults

none

Command Modes

INTERFACE VLAN

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The VLAN:

- can be in only one mode, either `community`, `isolated`, or `primary`.
- mode ode to `community` or `isolated` even before associating it to a primary VLAN. This secondary VLAN continues to work normally as a normal VLAN even though it is not associated to a primary VLAN. (A syslog message indicates this.)
- must not have a port in it when VLAN mode is being set.

Only ports (and port channels) configured as promiscuous, host, or PVLAN trunk ports (as previously described) can be added to the PVLAN. No other regular ports can be added to the PVLAN.

After using this command to configure a VLAN as a primary VLAN, use the `private-vlan mapping secondary-vlan` command to map secondary VLANs to this VLAN.

Related Commands

private-vlan mapping secondary-vlan — maps secondary VLANs to the selected primary VLAN.

show interfaces private-vlan — displays the type and status of the PVLAN interfaces.

show vlan private-vlan — displays the PVLANs and/or interfaces that are part of a PVLAN.

show vlan private-vlan mapping — displays the primary-secondary VLAN mapping.

switchport mode private-vlan — sets PVLAN mode of the selected port.

show interfaces private-vlan

Display type and status of PVLAN interfaces.

Syntax

`show interfaces private-vlan [interface interface]`

Parameters

interface *interface*	(OPTIONAL) Enter the keyword `interface` then the ID of the specific interface for which to display PVLAN status.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

This command has two types of display — a list of all PVLAN interfaces or for a specific interface. Examples of both types of output are shown below.

The following describes the `show interfaces private-vlan` command shown in the following examples.

Field	Description
Interface	Displays the type of interface and associated slot and port number.
Vlan	Displays the VLAN ID of the designated interface.
PVLAN-Type	Displays the type of VLAN in which the designated interface resides.
Interface Type	Displays the PVLAN port type of the designated interface.
Status	States whether the interface is operationally up or down.

Example (All)

```
Dell# show interfaces private-vlan
Interface Vlan PVLAN-Type Interface Type Status
--------- ---- ---------- -------------- --------
Gi 2/1    10   Primary    Promiscuous    Up
Gi 2/2    100  Isolated   Host           Down
Gi 2/3    10   Primary    Trunk          Up
Gi 2/4    101  Community  Host           Up
```

Example (Specific)

```
Dell# show interfaces private-vlan Gi 2/2
Interface Vlan PVLAN-Type Interface Type Status
--------- ---- ---------- -------------- --------
Gi 2/2    100  Isolated   Host           Up
```

Related Commands	private-vlan mode — sets the mode of the selected VLAN to community, isolated, or primary. show vlan private-vlan — displays the PVLANs and/or interfaces that are part of a PVLAN. show vlan private-vlan mapping — displays the primary-secondary VLAN mapping. switchport mode private-vlan — sets PVLAN mode of the selected port.

show vlan private-vlan

Display PVLANs and/or interfaces that are part of a PVLAN.

Syntax

```
show vlan private-vlan [community | interface | isolated |
primary | primary_vlan | interface interface]
```

Parameters

community	(OPTIONAL) Enter the keyword `community` to display VLANs configured as community VLANs, along with their interfaces.
interface	(OPTIONAL) Enter the keyword `interface` to display VLANs configured as community VLANs, along with their interfaces.
isolated	(OPTIONAL) Enter the keyword `isolated` to display VLANs configured as isolated VLANs, along with their interfaces.
primary	(OPTIONAL) Enter the keyword `primary` to display VLANs configured as primary VLANs, along with their interfaces.
primary_vlan	(OPTIONAL) Enter a private VLAN ID or secondary VLAN ID to display interface details about the designated PVLAN.
interface *interface*	(OPTIONAL) Enter the keyword `interface` and an interface ID to display the PVLAN configuration of the designated interface.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Examples of all types of command output are shown below. The first type of output is the result of not entering an optional keyword. It displays a detailed list of all PVLANs and their member VLANs and interfaces. The other types of output show details about PVLAN subsets.

The following describes the `show private-vlan` command shown in the Examples below.

Field	Description
Primary	Displays the VLAN ID of the designated or associated primary VLAN(s).
Secondary	Displays the VLAN ID of the designated or associated secondary VLAN(s).
Type	Displays the type of VLAN in which the listed interfaces reside.
Active	States whether the interface is operationally up or down.
Ports	Displays the interface IDs in the listed VLAN.

Example (All)

```
Dell# show vlan private-vlan
Primary Secondary Type      Active Ports
------- --------- --------- ------ -----------
10                primary   Yes    Gi 2/1,3
        100       isolated  Yes    Gi 2/2
        101       community Yes    Gi 2/10
20                primary   Yes    Po 10, 12-13
                                   Gi 3/1
        200       isolated  Yes    Gi 3/2,4-6
        201       community No
        202       community Yes    Gi 3/11-12
```

Example (Primary)

```
Dell# show vlan private-vlan primary
Primary Secondary Type    Active  Ports
------- --------- --------- ------ -------
10                primary  Yes    Gi 2/1,3
20                primary  Yes    Gi 3/1,3
```

Example (Isolated)

```
Dell# show vlan private-vlan isolated
Primary Secondary Type      Active Ports
------- --------- --------- ------ ----------
10                primary   Yes    Gi 2/1,3
        100       isolated  Yes    Gi 2/2,4-6
        200       isolated  Yes    Gi 3/2,4-6
```

Example (Community)

```
Dell# show vlan private-vlan community
Primary Secondary Type      Active Ports
------- --------- --------- ------ -----------
10                primary   Yes    Gi 2/1,3
        101       community Yes    Gi 2/7-10
20                primary   Yes    Po 10, 12-13
                                   Gi 3/1
        201       community No
        202       community Yes    Gi 3/11-12
```

Example (Specific)

```
Dell# show vlan private-vlan interface Gi 2/1
Primary Secondary Type     Active Ports
------- --------- --------- --------------------
10                primary  Yes    Gi 2/1
```

Usage Information

If the VLAN ID is that of a primary VLAN, the entire private VLAN output is displayed, as shown below. If the VLAN ID is a secondary VLAN, only its primary VLAN and its particular secondary VLAN properties are displayed, as shown in the second Example.

Example

```
Dell# show vlan private-vlan 10
Primary Secondary Type      Active  Ports
------- --------- --------- -------------------
10                primary   Yes     Gi 2/1,3
        102       isolated  Yes     Gi 0/4
        101       community Yes     Gi 2/7-10
```

Example

```
Dell#show vlan private-vlan 102
Primary Secondary Type     Active Ports
------- --------- --------- --------------------
10                Primary  Yes    Po 1
                                  Gi 0/2
        102       Isolated Yes    Gi 0/4
```

Related Commands

private-vlan mode — sets the mode of the selected VLAN to community, isolated, or primary.

show interfaces private-vlan — displays type and status of PVLAN interfaces.

show vlan private-vlan mapping — displays the primary-secondary VLAN mapping.

switchport mode private-vlan — sets PVLAN mode of the selected port.

show vlan private-vlan mapping

Display primary-secondary VLAN mapping.

Syntax

`show vlan private-vlan mapping`

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced the on MXL 10/40GbE Switch IO Module.

Usage Information

The output of this command, shown below, displays the community and isolated VLAN IDs that are associated with each primary VLAN.

Example

```
Dell# show vlan private-vlan mapping
Private Vlan:
  Primary   : 100
  Isolated  : 102
  Community : 101
  Unknown   : 200
```

Related Commands	private-vlan mode — sets the mode of the selected VLAN to community, isolated, or primary. show vlan private-vlan — displays type and status of PVLAN interfaces. show vlan private-vlan mapping — displays the primary-secondary VLAN mapping. switchport mode private-vlan — sets PVLAN mode of the selected port.

switchport mode private-vlan

Set PVLAN mode of the selected port.

Syntax

`[no] switchport mode private-vlan {host | promiscuous | trunk}`

To remove PVLAN mode from the selected port, use the `no switchport mode private-vlan` command.

Parameters

host	Enter the keyword `host` to configure the selected port or port channel as an isolated interface in a PVLAN.
promiscuous	Enter the keyword `promiscuous` to configure the selected port or port channel as an promiscuous interface.
trunk	Enter the keyword `trunk` to configure the selected port or port channel as a trunk port in a PVLAN.

Defaults

Disabled.

Command Modes

INTERFACE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The assignment of the various PVLAN port types to port and port channel (LAG) interfaces is shown in the following example.

Example

```
Dell#conf
Dell(conf)#interface GigabitEthernet 2/1
Dell(conf-if-gi-2/1)#switchport mode private-vlan promiscuous

Dell(conf)#interface GigabitEthernet 2/2
Dell(conf-if-gi-2/2)#switchport mode private-vlan host

Dell(conf)#interface GigabitEthernet 2/3
Dell(conf-if-gi-2/3)#switchport mode private-vlan trunk

Dell(conf)#interface port-channel 10
Dell(conf-if-gi-2/3)#switchport mode private-vlan promiscuous
```

Related Commands	private-vlan mode — sets the mode of the selected VLAN to community, isolated, or primary. private-vlan mapping secondary-vlan — sets the mode of the selected VLAN to primary and then associates the secondary VLANs to it. show interfaces private-vlan — displays type and status of PVLAN interfaces. show vlan private-vlan mapping — displays the primary-secondary VLAN mapping.

42

Per-VLAN Spanning Tree Plus (PVST+)

The Dell Networking Operating System (OS) implementation of per-VLAN spanning tree plus (PVST+) is based on the IEEE 802.1w standard spanning tree protocol, but it creates a separate spanning tree for each VLAN configured.

NOTE: For easier command line entry, the plus (+) sign is not used at the command line.

description

Enter a description of the PVST+.

Syntax	`description {`*`description`*`}` To remove the description, use the `no description {`*`description`*`}` command.
Parameters	*description* — Enter a description to identify the spanning tree (80 characters maximum).
Defaults	none
Command Modes	SPANNING TREE PVST+ (The prompt is “config-pvst”.)
Command History	Version 8.3.16.1 — Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	protocol spanning-tree pvst — enter SPANNING TREE mode on the switch.

disable

Disable PVST+ globally.

Syntax	`disable` To enable PVST+, use the `no disable` command.
Defaults	Disabled.

Command Modes	CONFIGURATION (conf-pvst)
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	protocol spanning-tree pvst — enter PVST+ mode.

edge-port bpdufilter default

Enable BPDU Filter globally to filter transmission of BPDU on port fast enabled interfaces.

Syntax	`edge-port bpdufilter default` To disable global bpdu filter default, use the `no edge-port bpdufilter default` command.
Defaults	Disabled
Command Modes	CONFIGURATION (The prompt is "config-pvst".)
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

extend system-id

To augment the Bridge ID with a VLAN ID so that PVST+ differentiate between BPDUs for each VLAN, use extend system ID. If the VLAN receives a BPDU meant for another VLAN, PVST+ does not detect a loop, and both ports can remain in Forwarding state.

Syntax	`extend system-id`
Defaults	Disabled
Command Modes	PROTOCOL PVST
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell(conf-pvst)#do show spanning-tree pvst vlan 2 brief
VLAN 2
Executing IEEE compatible Spanning Tree Protocol
Root ID    Priority 32768, Address 001e.c9f1.00f3
Root Bridge hello time 2, max age 20, forward delay 15
Bridge ID  Priority 32768, Address 001e.c9f1.00f3
We are the root of Vlan 2
Configured hello time 2, max age 20, forward delay 15
Bpdu filter disabled globally
```

```
Interface                                Designated
Name  PortID  Prio Cost  Sts  Cost Bridge ID
PortID
---------- --------- ---- ------ ----------- -------
-------------------- ---------
Po 23 128.24  128  1600  FWD  0    32768
001e.c9f1.00f3 128.24
Te 5/41 128.450 128 2000 DIS  0    32768
001e.c9f1.00f3 128.450
Te 5/50 128.459 128 2000 FWD  0    32768
001e.c9f1.00f3 128.459

Interface
Name    Role  PortID  Prio  Cost  Sts  Cost Link-type
Edge BpduFilter
---------- ------ -------- ---- ---- ---------
---- ----------
Po 23   Desg  128.24  128  1600  FWD  0   P2P No
No
Te 5/41 Dis   128.450 128  2000  DIS  0   P2P No
No
Te 5/50 Desg  128.459 128  2000  FWD  0   P2P No
No
```

Related Commands

protocol spanning-tree pvst — enter SPANNING TREE mode on the switch.

protocol spanning-tree pvst

To enable PVST+ on a device, enter the PVST+ mode.

Syntax

`protocol spanning-tree pvst`

To disable PVST+, use the `disable` command.

Defaults

none

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#conf
Dell(conf)#protocol spanning-tree pvst
Dell(conf-pvst)#no disable
Dell(conf-pvst)#vlan 2 bridge-priority 4096
Dell(conf-pvst)#vlan 3 bridge-priority 16384
Dell(conf-pvst)#
Dell(conf-pvst)#show config
!
protocol spanning-tree pvst
  no disable
  vlan 2 bridge-priority 4096
  vlan 3 bridge-priority 16384
Dell#
```

Usage Information	After you enable PVST+, the device runs an STP instance for each VLAN it supports.
Related Commands	disable — disables PVST+. show spanning-tree pvst — displays the PVST+ configuration.

show spanning-tree pvst

View the Per-VLAN spanning tree configuration.

Syntax

`show spanning-tree pvst [vlan vlan-id] [brief] [guard]`

Parameters

vlan *vlan-id*	(OPTIONAL) Enter the keyword `vlan` then the VLAN ID. The range is 1 to 4094.
brief	(OPTIONAL) Enter the keyword `brief` to view a synopsis of the PVST+ configuration information.
interface	(OPTIONAL) Enter one of the interface keywords along with the slot/port information: • For a Port Channel interface, enter the keyword `port-channel` then a number: The range is 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
guard	(OPTIONAL) Enter the keyword `guard` to display the type of guard enabled on a PVST interface and the current port state.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show spanning-tree pvst` command shown in the following examples.

Field	Description
Interface Name	PVST interface.
Instance	PVST instance.

Field	Description
Sts	Port state: root-inconsistent (INCON Root), forwarding (FWD), listening (LIS), blocking (BLK), or shut down (EDS Shut).
Guard Type	Type of STP guard configured (Root, Loop, or BPDU guard).
Bpdu Filter	Yes - Bpdu filter Enabled No - Bpdu filter Disabled

Example (Brief)

```
Dell# show spanning-tree pvst vlan 2 brief
VLAN 2
Executing IEEE compatible Spanning Tree Protocol
Root ID Priority 32768, Address 001e.c9f1.00f3
Root Bridge hello time 2, max age 20, forward delay 15
Bridge ID Priority 32768, Address 001e.c9f1.00f3
We are the root of Vlan 2
Configured hello time 2, max age 20, forward delay 15
Bpdu filter disabled globally

Interface                             Designated
Name    PortID  Prio Cost  Sts  Cost Bridge ID
PortID
---------- -------- ---- ------- --- -------
---------------------
Po 23   128.24  128  1600  FWD  0    32768 001e.c9f1.00f3
128.24
Te 5/41 128.450 128  2000  DIS  0    32768 001e.c9f1.00f3
128.450
Te 5/50 128.459 128  2000  FWD  0    32768 001e.c9f1.00f3
128.459

Interface                                            Bpdu
Name      Role  PortID  Prio Cost  Sts  Cost Link-type Edge
Filter
---------- ------ -------- ---- ------- --- -------- ----
------
Po 23     Desg  128.24  128  1600  FWD  0    P2P      No    No
Te 5/41   Dis   128.450 128  2000  DIS  0    P2P      No    No
Te 5/50   Desg  128.459 128  2000  FWD  0    P2P      No    No
Dell#
```

Example

```
Dell#show spanning-tree pvst vlan 2
VLAN 2
Root Identifier has priority 32768, Address 001e.c9f1.00f3
Root Bridge hello time 2, max age 20, forward delay 15
Bridge Identifier has priority 32768, Address 001e.c9f1.00f3
Configured hello time 2, max age 20, forward delay 15
Bpdu filter disabled globally
We are the root of VLAN 2
Current root has priority 32768, Address 001e.c9f1.00f3
Number of topology changes 0, last change occurred 3d1h ago on

Port 24 (Port-channel 23) is designated Discarding
Port path cost 1600, Port priority 128, Port Identifier 128.24
Designated root has priority 32768, address 001e.c9f1.00:f3
Designated bridge has priority 32768, address 001e.c9f1.00:f3
Designated port id is 128.24 , designated path cost 0
```

```
Number of transitions to forwarding state 0
BPDU sent 8, received 0
The port is not in the Edge port mode, bpdu filter is disabled

Port 450 (TenGigabitEthernet 5/41) is disabled Discarding
Port path cost 2000, Port priority 128, Port Identifier 128.450
Designated root has priority 32768, address 001e.c9f1.00:f3
Designated bridge has priority 32768, address 001e.c9f1.00:f3
Designated port id is 128.450 , designated path cost 0
Number of transitions to forwarding state 0
BPDU sent 0, received 0
The port is not in the Edge port mode, bpdu filter is disabled

Port 459 (TenGigabitEthernet 5/50) is designated Forwarding
Port path cost 2000, Port priority 128, Port Identifier 128.459
Designated root has priority 32768, address 001e.c9f1.00:f3
Designated bridge has priority 32768, address 001e.c9f1.00:f3
Designated port id is 128.459 , designated path cost 0
Number of transitions to forwarding state 1
BPDU sent 16, received 0
The port is not in the Edge port mode, bpdu filter is disabled
```

Example (EDS/LBK)

```
Dell#show spanning-tree pvst vlan 2 interface gigabitethernet
1/0
```

GigabitEthernet 1/0 of VLAN 2 is LBK_INC discarding

```
Edge port:no (default) port guard :none (default)
Link type: point-to-point (auto) bpdu filter:disable (default)
Bpdu guard :disable (default)
Bpdus sent 152, received 27562

Interface Designated
Name    PortID   Prio Cost  Sts Cost Bridge ID       PortID
-----------------------------------------------------------
Gi 1/0  128.1223 128  20000 EDS 0 32768 0001.e800.a12b 128.1223
```

Example (EDS/PVID)

```
Dell#show spanning-tree pvst vlan 2 interface gigabitethernet
1/0
```

GigabitEthernet 1/0 of VLAN 2 is PVID_INC discarding

```
Edge port:no (default) port guard :none (default)
Link type: point-to-point (auto) bpdu filter:disable (default)
Bpdu guard :disable (default)
Bpdus sent 1, received 0

Interface Designated
Name   PortID   Prio Cost  Sts Cost Bridge ID       PortID
---------------------------------------------------------
Gi 1/0 128.1223 128 20000 EDS 0 32768 0001.e800.a12b 128.1223
```

Example (Guard)

```
Dell#show spanning-tree pvst vlan 5 guard

Interface
Name       Instance Sts       Guard type Bpdu Filter
--------- -------- --------- ---------- -----------
TenGig 0/1 0      INCON(Root) Rootguard   No
TenGig 0/2 0      FWD         Loopguard   No
TenGig 0/3 0      EDS(Shut)   Bpduguard   No
```

Related Commands

spanning-tree pvst — configure PVST+ on an interface.

spanning-tree pvst

Configure a PVST+ interface with one of these settings: edge port with optional bridge port data unit (BPDU) guard, port disablement if an error condition occurs, port priority or cost for a VLAN range, loop guard, or root guard.

Syntax

```
spanning-tree pvst {edge-port [bpduguard [shutdown-on-
violation]] | bpdufilter] | err-disable | vlan vlan-range {cost
number | priority value} | rootguard}
```

Parameters

edge-port	Enter the keywords `edge-port` to configure the interface as a PVST+ edge port.
bpduguard	Enter the keyword `portfast` to enable Portfast to move the interface into Forwarding mode immediately after the root fails. Enter the keyword `bpduguard` to disable the port when it receives a BPDU.
shutdown-on-violation	(OPTIONAL) Enter the keywords `shutdown-on-violation` to hardware disable an interface when a BPDU is received and the port is disabled.
bpdufilter	(OPTIONAL) Enter the keyword `bpdufilter` to stop sending and receiving BPDUs on port fast enabled ports.
err-disable	Enter the keywords `err-disable` to enable the port to be put into the error-disable state (EDS) if an error condition occurs.
vlan *vlan-range*	Enter the keyword `vlan` then the VLAN numbers. The range is from 1 to 4094.
cost *number*	Enter the keyword `cost` then the port cost value. The range is from 1 to 200000. Defaults: • 10-Gigabit Ethernet interface = **2000**. • 40-Gigabit Ethernet interface = **1400**. • Port Channel interface with one 10 Gigabit Ethernet = **2000**. • Port Channel with two 10 Gigabit Ethernet = **1800**. • Port Channel with two 40 Mbps Ethernet = **600**.

priority *value*	Enter the keyword `priority` then the Port priority value in increments of 16. The range is from 0 to 240. The default is **128**.
rootguard	Enter the keyword `rootguard` to enable root guard on a PVST+ port or port-channel interface.

Defaults Not configured.

Command Modes INTERFACE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information The BPDU guard option prevents the port from participating in an active STP topology in case a BPDU appears on a port unintentionally, or is misconfigured, or is subject to a DOS attack. This option places the port into the Error Disable state if a BPDU appears, and a message is logged so that the administrator can take corrective action. When BPDU guard and BPDU filter is enabled on the port, then BPDU filter takes the highest precedence.

NOTE: A port configured as an edge port, on a PVST switch, will immediately transition to the forwarding state. Only ports connected to end-hosts should be configured as an edge port. Consider an edge port similar to a port with a spanning-tree portfast enabled.

Example

```
Dell(conf-if-gi-1/1)#spanning-tree pvst vlan 3 cost 18000
Dell(conf-if-gi-1/1)#end
Dell(conf-if-gi-1/1)#show config
!
interface GigabitEthernet 1/1
  no ip address
  switchport
  spanning-tree pvst vlan 3 cost 18000
  no shutdown
Dell(conf-if-gi-1/1)#end

Dell#
```

Related Commands show spanning-tree pvst — views the PVST+ configuration.

spanning-tree pvst err-disable

Place ports in an Err-Disabled state if they receive a PVST+ BPDU when they are members an untagged VLAN.

Syntax `spanning-tree pvst err-disable cause invalid-pvst-bpdu`

Defaults Enabled; ports are placed in the Err-Disabled state if they receive a PVST+ BPDU when they are members of an untagged VLAN.

Command Modes	INTERFACE
Command History	**Version 8.3.16.1** Introduced on MXL 10/40GbE Switch IO Module
Usage Information	Some non-Dell Networking systems which have hybrid ports participating in PVST+ transmit two kinds of BPDUs: an 802.1D BPDU and an untagged PVST+ BPDU. Dell Networking systems do not expect PVST+ BPDU on an untagged port. If this happens, the system places the port in the Error-Disable state. This behavior might result in the network not converging. To prevent the system from executing this action, use the `no spanning-tree pvst err-disable` command `cause invalid-pvst-bpdu`.
Related Commands	show spanning-tree pvst — views the PVST+ configuration.

tc-flush-standard

Enable the MAC address flushing after receiving every topology change notification.

Syntax	`tc-flush-standard` To disable, use the `no tc-flush-standard` command.
Defaults	Disabled.
Command Modes	CONFIGURATION
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	By default, the system implements an optimized flush mechanism for PVST+. This implementation helps in flushing the MAC addresses only when necessary (and less often) allowing for faster convergence during topology changes. However, if a standards-based flush mechanism is needed, you can turn this *knob* command on to enable flushing MAC addresses after receiving every topology change notification.

vlan bridge-priority

Set the PVST+ bridge-priority for a VLAN or a set of VLANs.

Syntax	`vlan` *`vlan-id`* `bridge-priority` *`value`* To return to the default value, use the `no vlan bridge-priority` command.

Parameters

vlan *vlan-range*	Enter the keyword `vlan` then the VLAN numbers. The range is from 1 to 4094.
bridge-priority *value*	Enter the keywords `bridge-priority` then the bridge priority value in increments of 4096. The range is from 0 to 61440. The default is **32768**.

Defaults **32768**

Command Modes CONFIGURATION (conf-pvst)

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

vlan forward-delay — changes the time interval before the system transitions to the Forwarding state.

vlan hello-time — change the time interval between BPDUs.

vlan max-age — changes the time interval before PVST+ refreshes.

show spanning-tree pvst — displays the PVST+ configuration.

vlan forward-delay

Set the amount of time the interface waits in the Listening state and the Learning state before transitioning to the Forwarding state.

Syntax `vlan vlan-id forward-delay seconds`

To return to the default setting, use the `no vlan forward-delay` command.

Parameters

vlan *vlan-range*	Enter the keyword `vlan` then the VLAN numbers. The range is from 1 to 4094.
forward-delay *seconds*	Enter the keywords `forward-delay` then the time interval, in seconds, that the system waits before transitioning PVST+ to the forwarding state. The range is from 4 to 30 seconds. The default is **15 seconds**.

Defaults **15 seconds**

Command Modes CONFIGURATION (conf-pvst)

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands	vlan bridge-priority — sets the bridge-priority value. vlan hello-time — changes the time interval between BPDUs. vlan max-age — changes the time interval before PVST+ refreshes. show spanning-tree pvst — displays the PVST+ configuration.

vlan hello-time

Set the time interval between generation of PVST+ and BPDUs.

Syntax

`vlan vlan-id hello-time seconds`

To return to the default value, use the `no vlan hello-time` command.

Parameters

vlan *vlan-range*	Enter the keyword `vlan` then the VLAN numbers. The range is from 1 to 4094.
hello-time *seconds*	Enter the keywords `hello-time` then the time interval, in seconds, between transmission of BPDUs. The range is from 1 to 10 seconds. The default is **2 seconds**.

Defaults

2 seconds

Command Modes

CONFIGURATION (conf-pvst)

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

vlan bridge-priority — sets the bridge-priority value.

vlan forward-delay — changes the time interval before the system transitions to the forwarding state.

vlan max-age — changes the time interval before PVST+ refreshes.

show spanning-tree pvst — displays the PVST+ configuration.

vlan max-age

To maintain configuration information before refreshing that information, set the time interval for the PVST+ bridge.

Syntax	`vlan vlan-range max-age seconds` To return to the default, use the `no vlan max-age` command.
Parameters	

vlan *vlan-range*	Enter the keyword `vlan` then the VLAN numbers. The range is from 1 to 4094.
max-age *seconds*	Enter the keywords `max-age` then the time interval, in seconds, that the system waits before refreshing configuration information. The range is from 6 to 40 seconds. The default is **20 seconds**.

Defaults	**20 seconds**
Command Modes	CONFIGURATION (conf-pvst)
Command History	

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

vlan bridge-priority — sets the bridge-priority value.

vlan forward-delay — changes the time interval before the system transitions to the forwarding state.

vlan hello-time — changes the time interval between BPDUs.

show spanning-tree pvst — displays the PVST+ configuration.

43

Quality of Service (QoS)

The Dell Networking Operating System (OS) commands for quality of service (QoS) include traffic conditioning and congestion control.

This chapter contains the following sections:

- Global Configuration Commands
- Per-Port QoS Commands
- Policy-Based QoS Commands

Global Configuration Commands

There are only two global configuration QoS commands.

qos-rate-adjust

By default, while rate limiting, policing, and shaping, the system does not include the Preamble, SFD, or the IFG fields. These fields are overhead; only the fields from MAC destination address to the CRC are used for forwarding and are included in these rate metering calculations. You can optionally include overhead fields in rate metering calculations by enabling QoS Rate Adjustment.

Syntax

`qos-rate-adjustment overhead-bytes`

Parameters

overhead-bytes	Include a specified number of bytes of packet overhead to include in rate limiting, policing, and shaping calculations. The range is from 1 to 31.

Defaults

QoS rate adjustment is disabled by default, and `no qos-rate-adjust` is listed in the running-configuration

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

service-class dot1p-mapping

This command maps an 802.1p priority to an internal traffic class.

Syntax	`service-class dot1p-mapping user-priority`
Parameters	*user-priority* — The user-priority value ranges from 0 to 7.
Command Modes	CONFIGURATION
Command History	Version 8.3.16.1 — Introduced on the MXL 10/40GbE Switch IO Module.

Per-Port QoS Commands

Per-port QoS (port-based QoS) allows you to define the QoS configuration on a per-physical-port basis.

dot1p-priority

Assign a value to the IEEE 802.1p bits on the traffic this interface receives.

Syntax

```
dot1p-priority priority-value
```

To delete the IEEE 802.1p configuration on the interface, use the `no dot1p-priority` command.

Parameters

priority-value	Enter a value from 0 to 7.

dot1p	Queue Number
0	0
1	0
2	0
3	1
4	2
5	3
6	3
7	3

Defaults none

Command Modes	INTERFACE
Command History	**Version 9.2(0.0)** Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only. **Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	The `dot1p-priority` command changes the priority of incoming traffic on the interface. The system places traffic marked with a priority in the correct queue and processes that traffic according to its queue. When you set the priority for a port channel, the physical interfaces assigned to the port channel are configured with the same value. You cannot assign the `dot1p-priority` command to individual interfaces in a port channel.

rate police

Police the incoming traffic rate on the selected interface.

Syntax

```
rate police [kbps] committed-rate [burst-KB] [peak [kbps] peak-rate [burst-KB]] [vlan vlan-id]
```

Parameters

kbps	Enter the keyword `kbps` to specify the rate limit in Kilobits per second (Kbps). Make the following value a multiple of 64. The range is from 0 to 40000000. The default granularity is Megabits per second (Mbps).
committed-rate	Enter the bandwidth in Mbps. The range is from 0 to 10000.
burst-KB	(OPTIONAL) Enter the burst size in KB. The range is from 16 to 200000. The default is **50**.
peak *peak-rate*	(OPTIONAL) Enter the keyword `peak` then a number to specify the peak rate in Mbps. The range is from 0 to 10000.
vlan *vlan-id*	(OPTIONAL) Enter the keyword `vlan` then a VLAN ID to police traffic to those specific VLANs. The range is from 1 to 4094.

Defaults	Granularity for `commited-rate` and `peak-rate` is Mbps unless you use the `kbps` option.
Command Modes	INTERFACE
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

NOTE: Per port rate police is supported for Layer 2 tagged and untagged switched traffic and for Layer 3 traffic. Per VLAN rate police is supported on only tagged ports with Layer 2 switched traffic.

On one interface, you can configure the `rate police` command for a VLAN or you can configure the `rate police` command for an interface. For each physical interface, you can configure three `rate police` commands specifying different VLANS.

For each physical interface, you can configure three `rate police` commands specifying different VLANs.

Related Commands

rate-police — specifies traffic policing on the selected interface.

rate shape

Shape the traffic output on the selected interface.

Syntax

```
rate shape [kbps] rate [burst-KB]
```

Parameters

kbps	Enter the keyword `kbps` to specify the rate limit in Kilobits per second (Kbps). Make the following value a multiple of 64. The range is from 0 to 40000000. The default granularity is Megabits per second (Mbps).
rate	Enter the outgoing rate in multiples of 10 Mbps. The range is from 10 to 10000.
burst-KB	(OPTIONAL) Enter the burst size in KB. The range is from 0 to 10000. The default is **50**.

Defaults

Granularity for rate is **Mbps** unless you use the `kbps` option.

Command Modes

INTERFACE

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

rate-shape — shapes traffic output as part of the designated policy.

service-class dynamic dot1p

Honor all 802.1p markings on incoming switched traffic on an interface (from INTERFACE mode) or on all interfaces (from CONFIGURATION mode). A CONFIGURATION mode entry supersedes an INTERFACE mode entry.

Syntax

```
service-class dynamic dot1p
```

To return to the default setting, use the `no service-class dynamic dot1p` command.

Defaults

All dot1p traffic is mapped to Queue 0 unless you enable the `service-class dynamic dot1p` command. The default mapping is as follows:

dot1p	Queue ID
0	0
1	0
2	0
3	1
4	2
5	3
6	3
7	3

Command Modes

- INTERFACE
- CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To honor all incoming 802.1p markings on incoming switched traffic on the interface, enter this command. By default, this facility is not enabled (that is, the 802.1p markings on incoming traffic are not honored).

You can apply this command on both physical interfaces and port channels. When you set the service-class dynamic for a port channel, the physical interfaces assigned to the port channel are automatically configured; you cannot assign the `service-class dynamic` command to individual interfaces in a port channel.

- All dot1p traffic is mapped to Queue 0 unless you enable the `service-class dynamic dot1p` command on an interface or globally.
- Layer 2 or Layer 3 service policies supersede dot1p service classes.

service-class bandwidth-percentage

Specify a minimum bandwidth for queues.

Syntax

```
service-class bandwidth-percentage queue0 number queue1 number
queue2 number queue3 number
```

Parameters

number	Enter the bandwidth-weight, as a percentage. The range is from 1 to 100.

Defaults

none

Command Modes

CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Guarantee a minimum bandwidth to different queues globally using the `service-class bandwidth-percentage` command from CONFIGURATION mode. The command is applied in the same way as the `bandwidth-percentage` command in an output QoS policy. The `bandwidth-percentage` command in QOS-POLICY-OUT mode supersedes the `service-class bandwidth-percentage` command.

When you enable ETS, the egress QoS features in the output QoS policy-map (such as `service-class bandwidth-percentage` and `bandwidth-percentage`), the default bandwidth allocation ratio for egress queues are superseded by ETS configurations. This is to provide compatibility with DCBX. Therefore, Dell Networking OS recommends disabling ETS when you wish to apply these features exclusively. After you disable ETS on an interface, the configured parameters are applied.

strict-priority unicast

Configure a unicast queue as a strict-priority (SP) queue.

Syntax

```
strict-priority unicast queue number
```

Parameters

unicast *number*	Enter the keyword `unicast` then the queue number. The range is from 1 to 3.

Defaults

none

Command Modes

CONFIGURATION

Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	After you configure a unicast queue as strict-priority, that particular queue, on the entire chassis, is treated as a `strict-priority queue`. Traffic for a strict priority is scheduled before any other queues are serviced. For example, if you send 100% line rate traffic over the SP queue, it starves all other queues on the ports on which this traffic is flowing. To assign the strict priority schedule type to egress queues, use the `scheduler strict` command in QOS-POLICY-OUT mode. The system OS does not support bandwidth configuration on strict priority scheduler queues. When you enable ETS, the egress QoS features in the output QoS policy-map (such as `strict priority unicast <0-3>` and `scheduler strict`), default scheduler for egress queues are superseded by ETS configurations. This is to provide compatibility with DCBX. Therefore, Dell Networking OS recommends disabling ETS when you wish to apply these features exclusively. After you disable ETS on an interface, the configured parameters are applied.

Policy-Based QoS Commands

Policy-based traffic classification is handled with class maps. These maps classify unicast traffic into one of four classes. The system allows you to match multiple class maps and specify multiple match criteria. Policy-based QoS is not supported on logical interfaces, such as port-channels, VLANs, or Loopbacks.

bandwidth-percentage

Assign a percentage of weight to the class/queue.

Syntax	`bandwidth-percentage` *`percentage`* To remove the bandwidth percentage, use the `no bandwidth-percentage` command.	
Parameters	*percentage*	Enter the percentage assignment of weight to the class/queue. The range is from 1 to 100% (granularity 1%).
Defaults	none	
Command Modes	CONFIGURATION (conf-qos-policy-out)	
Command History	Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information	The unit of bandwidth percentage is 1%. If the sum of the bandwidth percentages given to all eight classes exceeds 100%, the bandwidth percentage automatically scales down to 100%.
Related Commands	qos-policy-output — creates a QoS output policy.

class-map

Create/access a class map. Class maps differentiate traffic so that you can apply separate quality-of-service policies to each class.

Syntax

```
class-map {match-all | match-any} class-map-name [layer2]
```

Parameters

match-all	Determines how packets are evaluated when multiple match criteria exist. Enter the keywords `match-all` to determine that the packets must meet all the match criteria in order to be a member of the class.
match-any	Determines how packets are evaluated when multiple match criteria exist. Enter the keywords `match-any` to determine that the packets must meet at least one of the match criteria in order to be a member of the class.
class-map-name	Enter a name of the class for the class map in a character format (32 character maximum).
layer2	Enter the keyword `layer2` to specify a Layer 2 Class Map. The default is **Layer 3**.

Defaults	Layer 3
Command Modes	CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Packets arriving at the input interface are checked against the match criteria configured using this command to determine if the packet belongs to that class. This command accesses CLASS-MAP mode, where the configuration commands include the`match ip` and `match mac` options.

Related Commands

ip access-list extended — configures an extended IP ACL.

ip access-list standard — configures a standard IP ACL.

match ip access-group — configures the match criteria based on the access control list (ACL).

match ip precedence — identifies the IP precedence values as match criteria.

match ip dscp configures the match criteria based on the DSCP value.

match ip access-group — configures a match criterion for a class map based on the contents of the designated MAC ACL.

match mac dot1p — configures a match criterion for a class map based on a dot1p value.

match mac vlan — configures a match criterion for a class map based on VLAN ID.

service-queue — assigns a class map and QoS policy to different queues.

show qos class-map — views the current class map information.

clear qos statistics

Clears matched packets.

Syntax	`clear qos statistics` *`interface-name`*

Parameters

interface-name	Enter one of the following keywords: • For a 40-Gigabit Ethernet interface, enter the keyword `FortyGigabitEthernet` then the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.

Defaults: none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

When you issue this command, statistical information stored regarding QoS clears and resets to 0. You can access these statistics using the `show qos statistics` command in EXEC mode. When the traffic pattern matches the QoS classification criteria flows, the corresponding counters increment.

Related Commands

show qos statistics — displays the QoS statistics.

crypto key zeroize rsa

Removes the generated RSA host keys and zeroize the key storage location.

Syntax	`crypto key zeroize rsa`
Defaults	none
Command Modes	CONFIGURATION
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide.* The following is a list of the Dell Networking OS version history for this command. Version 9.5(0.0) — Introduced on the Z9000, S6000, S4820T, S4810, MXL
Related Commands	crypto key generate — Generate keys for SSH server

ip ssh rekey

Configures the time rekey-interval or volume rekey-limit threshold at which to re-generate the SSH key during an SSH session.

Syntax	`ip ssh rekey [time rekey-interval] [volume rekey-limit]` To reset to the default, use `no ip ssh rekey [time rekey-interval] [volume rekey-limit]` command.

Parameters

time *minutes*	Enter the keywords `time` then the amount of time in minutes. The range is from 10 to 1440 minutes. The default is **60** minutes
volume *rekey-limit*	Enter the keywords **volume** then the amount of volume in megabytes. The range is from 1 to 4096 to megabytes. The default is **1024 megabytes**

Defaults	The default time is **60** minutes. The default volume is **1024** megabytes.
Command Modes	CONFIGURATION mode

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version 9.5(0.0)	Introduced on the Z9000, S6000, S4820T, S4810, MXL

match ip access-group

Configure match criteria for a class map, based on the access control list (ACL).

Syntax

`match ip access-group access-group-name [set-ip-dscp value]`

To remove ACL match criteria from a class map, use the `no match ip access-group access-group-name [set-ip-dscp value]` command.

Parameters

access-group-name	Enter the ACL name whose contents are used as the match criteria in determining if packets belong to the class the `class-map` specifies.
set-ip-dscp *value*	(OPTIONAL) Enter the keywords `set-ip-dscp` then the IP DSCP value. The matched traffic is marked with the DSCP value. The range is from 0 to 63.

Defaults

none

Command Modes

CLASS-MAP CONFIGURATION (config-class-map)

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To access this command, enter the `class-map` command. After the class map is identified, you can configure the match criteria. For class-map match-any, a maximum of five ACL match criteria are allowed. For `class-map match-all`, only one ACL match criteria is allowed.

Related Commands

class-map — identifies the class map.

match ip vlan

Uses a VLAN as the match criterion for an L3 class map.

Syntax

`match ip vlan vlan-id`

To remove VLAN as the match criterion, use the `no match ip vlan vlan-id` command.

Parameters

vlan *vlan-id*	Enter the keyword vlan and then the ID of the VLAN. The range is from 1 to 4094.

Defaults

none

Command Modes

CONF-CLASS-MAP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version 9.4(0.0)	Introduced on the MXL switch.

Usage Information

To access this command, enter the `class-map` command. After the class map is identified, you can configure the match criteria.

Use this command to match an IP class-map against a single VLAN ID .

Related Commands

class-map — identifies the class map.

match ip vrf

Uses a VRF as the match criterion for an L3 class map.

Syntax

`match ip vrf vrf-id`

To remove VRF as the match criterion, use the `no match ip vrf vrf-id` command.

Parameters

vlan *vlan-id*	Enter the keyword `vrf` and then the ID of the VRF. The range is from 1 to 63.

Defaults

none

Command Modes

CONF-CLASS-MAP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version 9.4(0.0)	Introduced on the MXL switch.

Usage Information

To access this command, enter the `class-map` command. After the class map is identified, you can configure the match criteria.

Use this command to match an IP class-map against a single VRF ID .

Related Commands	class-map — identifies the class map.

description

Add a description to the selected policy map or QoS policy.

Syntax

`description {description}`

To remove the description, use the `no description {description}` command.

Parameters

description	Enter a description to identify the policies (80 characters maximum).

Defaults

none

Command Modes

CONFIGURATION (policy-map-input and policy-map-output; conf-qos-policy-in and conf-qos-policy-out; wred)

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

policy-map-output — creates an output policy map.

qos-policy-output — creates an output QoS-policy on the router.

match ip dscp

Use a differentiated services code point (DSCP) value as a match criteria.

Syntax

`match {ip | ipv6 | ip-any} dscp dscp-list [set-ip-dscp value]`

To remove a DSCP value as a match criteria, use the `no match {ip | ipv6 | ip-any} dscp dscp-list [[multicast] set-ip-dscp value]` command.

Parameters

ip	Enter the keyword `ip` to support IPv4 traffic.
ipv6	Enter the keyword `ipv6` to support IPv6 traffic
ip-any	Enter the keyword `ip-any` to support IPv4 and IPv6 traffic.

dscp-list	Enter the IP DSCP values that is to be the match criteria. Separate values by commas — no spaces (1,2,3) or indicate a list of values separated by a hyphen (1-3). The range is from 0 to 63.
set-ip-dscp *value*	(OPTIONAL) Enter the keywords `set-ip-dscp` then the IP DSCP value. The matched traffic is marked with the DSCP value. The range is from 0 to 63.

Defaults

none

Command Modes

CLASS-MAP CONFIGURATION (config-class-map)

Command History

Version 9.5(0.0)	Introduced the **ipv6** and **ip-any** options on the MXL 10/40GbE Switch.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To access this command, enter the `class-map` command. After the class map is identified, you can configure the match criteria.

The `match ip dscp` and `match ip precedence` commands are mutually exclusive.

Up to 64 IP DSCP values can be matched in one match statement. For example, to indicate IP DCSP values 0 1 2 3 4 5 6 7, enter either the `match ip dscp 0,1,2,3,4,5,6,7` or `match ip dscp 0-7` command.

NOTE: Only one of the IP DSCP values must be a successful match criterion, not all of the specified IP DSCP values must match.

Related Commands

class-map — identifies the class map.

match ip precedence

Use IP precedence values as a match criteria.

Syntax

`match {ip | ipv6 | ip-any} precedence ip-`*`precedence-list`*` [set-ip-dscp `*`value`*`]`

To remove IP precedence as a match criteria, use the `no match {ip | ipv6 | ip-any} precedence ip-`*`precedence-list`*` [[multicast] set-ip-dscp `*`value`*`]` command.

Parameters

ip	Enter the keyword `ip` to support IPv4 traffic.
ipv6	Enter the keyword `ipv6` to support IPv6 traffic.

ip-any	Enter the keyword `ip-any` to support IPv4 and IPv6 traffic.
ip-precedence-list	Enter the IP precedence value(s) as the match criteria. Separate values by commas — no spaces (1,2,3) or indicate a list of values separated by a hyphen (1-3). The range is from 0 to 7.
set-ip-dscp *value*	(OPTIONAL) Enter the keywords `set-ip-dscp` then the IP DSCP value. The matched traffic is marked with the DSCP value. The range is from 0 to 63.

Defaults none

Command Modes CLASS-MAP CONFIGURATION (config-class-map)

Command History

Version 9.5(0.0)	Introduced the support for ipv6 and ip-any options on the MXL 10/40GbE Switch.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To access this command, enter the `class-map` command. After the class map is identified, you can configure the match criteria.

The `match ip precedence` command and the `match ip dscp` command are mutually exclusive.

Up to eight precedence values can be matched in one match statement. For example, to indicate the IP precedence values 0 1 2 3, enter either the `match ip precedence 0-3` or `match ip precedence 0,1,2,3` command.

NOTE: Only one of the IP precedence values must be a successful match criterion, not all of the specified IP precedence values must match.

Related Commands class-map — identifies the class map.

match mac access-group

Configure a match criterion for a class map, based on the contents of the designated MAC ACL.

Syntax `match mac access-group {mac-acl-name}`

Parameters

mac-acl-name	Enter a MAC ACL name. Its contents is used as the match criteria in the class map.

Defaults none

Command Modes	CLASS-MAP
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	To access this command, enter the `class-map` command. After the class map is identified, you can configure the match criteria.
Related Commands	class-map — identifies the class map.

match mac dot1p

Configure a match criterion for a class map based on a dot1p value.

Syntax	`match mac dot1p {dot1p-list}`
Parameters	*dot1p-list* Enter a dot1p value. The range is from 0 to 7.
Defaults	none
Command Modes	CLASS-MAP
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	To access this command, enter the `class-map` command. After the class map is identified, you can configure the match criteria.
Related Commands	class-map — identifies the class map.

match mac vlan

Configure a match criterion for a class map based on VLAN ID.

Syntax	`match mac vlan number`
Parameters	*number* Enter the VLAN ID. The range is from 1 to 4094.
Defaults	none
Command Modes	CLASS-MAP

Command History	**Version 8.3.16.1**	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To access this command, enter the `class-map` command. You can match against only one VLAN ID.

Related Commands

class-map — identifies the class map.

policy-aggregate

Allow an aggregate method of configuring per-port QoS via policy maps. An aggregate QoS policy is part of the policy map (input/output) applied on an interface.

Syntax

`policy-aggregate` *`qos-policy-name`*

To remove a policy aggregate configuration, use the `no policy-aggregate` *`qos-policy-name`* command.

Parameters

qos-policy-name	Enter the name of the policy map in character format (32 characters maximum).

Defaults

none

Command Modes

CONFIGURATION (policy-map-input and policy-map-output)

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Aggregate input/output QoS policy applies to all the port ingoing/outgoing traffic. Aggregate input/output QoS policy can coexist with per queue input/output QoS policies.

1. If only aggregate input QoS policy exists, input traffic conditioning configurations (rate-police) apply. Any marking configurations in aggregate input QoS policy are ignored.
2. If aggregate input QoS policy and per class input QoS policy coexist, aggregate input QoS policy preempts per class input QoS policy on input traffic conditioning (rate-police). In other words, if rate police configuration exists in the aggregate QoS policy, the rate police configurations in per class QoS are ignored. Marking configurations in per class input QoS policy still apply to each queue.

Related Commands

policy-map-output — creates an output policy map.

policy-map-input

Create an input policy map.

Syntax

`policy-map-input *policy-map-name* [layer2]`

To remove an input policy map, use the `no policy-map-input *policy-map-name* [layer2]` command.

Parameters

policy-map-name	Enter the name of the policy map in character format (32 characters maximum).
layer2	(OPTIONAL) Enter the keyword `layer2` to specify a Layer 2 Class Map. The default is **Layer 3**.

Defaults

Layer 3

Command Modes

CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The input policy map is used to classify incoming traffic to different flows using class-map, QoS policy, or incoming packets DSCP. This command enables Policy-Map-Input Configuration mode (conf-policy-map-in).

Related Commands

service-queue — assigns a class map and QoS policy to different queues.

policy-aggregate — allows an aggregate method of configuring per-port QoS using policy maps.

service-policy input — applies an input policy map to the selected interface.

policy-map-output

Create an output policy map.

Syntax

`policy-map-output *policy-map-name*`

To remove a policy map, use the `no policy-map-output *policy-map-name*` command.

Parameters

policy-map-name	Enter the name for the policy map in character format (32 characters maximum).

Defaults	none
Command Modes	CONFIGURATION
Command History	**Version 9.2(0.0)** Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only. **Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	To assign traffic to different flows using QoS policy, use the Output Policy map. This command enables Policy-Map-Output Configuration mode (conf-policy-map-out).
Related Commands	service-queue — assigns a class map and QoS policy to different queues. policy-aggregate — allows an aggregate method of configuring per-port QoS using policy maps. service-policy output — applies an output policy map to the selected interface.

qos-policy-input

Create a QoS input policy on the router.

Syntax

`qos-policy-input qos-policy-name [layer2]`

To remove an existing input QoS policy from the router, use the `no qos-policy-input qos-policy-name [layer2]` command.

Parameters

qos-policy-name	Enter the name for the policy map in character format (32 characters maximum).
layer2	(OPTIONAL) Enter the keyword `layer2` to specify a Layer 2 Class Map. The default is **Layer 3**.

Defaults	**Layer 3**
Command Modes	CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To specify the name of the input QoS policy, use this command. After the input policy is specified, rate-police is defined. This command enables Qos-Policy-Input Configuration mode — (conf-qos-policy-in).

When changing a Service-Queue configuration in a QoS policy map, all QoS rules are deleted and re-added automatically to ensure that the order of the rules is maintained. As a result, the Matched Packets value shown in the `show qos statistics` command is reset.

Related Commands	rate police — incoming traffic policing function.

qos-policy-output

Create a QoS output policy.

Syntax

`qos-policy-output` *`qos-policy-name`*

To remove an existing output QoS policy, use the `no qos-policy-output` *`qos-policy-name`* command.

Parameters

qos-policy-name	Enter your output QoS policy name in character format (32 characters maximum).

Defaults

none

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To specify the name of the output QoS policy, use this command. After the output policy is specified, rate-limit, bandwidth-percentage, and WRED can be defined. This command enables Qos-Policy-Output Configuration mode — (conf-qos-policy-out).

Related Commands

bandwidth-percentage — assigns weight to the class/queue percentage.

rate police

Police the incoming traffic rate on the selected interface.

Syntax

`rate police [kbps]` *`committed-rate`* `[`*`burst-KB`*`] [peak [kbps]` *`peak-rate`* `[`*`burst-KB`*`]]`

Parameters

kbps	Enter the keyword `kbps` to specify the rate limit in Kilobits per second (Kbps). Make the following value a multiple of 64.

	The range is from 0 to 40000000. The default granularity is Megabits per second (Mbps).
committed-rate	Enter the bandwidth in Mbps. The range is from 0 to 10000.
burst-KB	(OPTIONAL) Enter the burst size in KB. The range is from 16 to 200000. The default is **100**.
peak *peak-rate*	(OPTIONAL) Enter the keyword `peak` then a number to specify the peak rate in Mbps. The range is from 0 to 10000. The default is the same as designated for *`committed-rate`*.

Defaults Burst size is 100 KB. *`peak-rate`* is the same as *`committed-rate`*. Granularity for *`committed-rate`* and *`peak-rate`* is Mbps unless you use the *`kbps`* option.

Command Modes INTERFACE

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

rate police — specifies traffic policing on the selected interface.

qos-policy-input — creates a QoS output policy.

rate shape

Shape the traffic output on the selected interface.

Syntax `rate shape [kbps] rate [burst-KB]`

Parameters

kbps	Enter the keyword `kbps` to specify the rate limit in Kilobits per second (Kbps). Make the following value a multiple of 64. The range is from 0 to 40000000. The default granularity is Megabits per second (Mbps).
rate	Enter the outgoing rate in multiples of 10 Mbps. The range is from 10 to 10000.
burst-KB	(OPTIONAL) Enter the burst size in KB. The range is from 0 to 10000. The default is **50**.

Defaults Granularity for rate is **Mbps** unless you use the `kbps` option.

Command Modes QOS-POLICY-OUT

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

When you apply `rate-shape` in QoS policy both on the Queue Level and in Aggregate mode, the queue-based shaping occurs first then aggregate rate shaping.

Related Commands

rate shape — shapes traffic output as part of the designated policy.

service-policy input

Apply an input policy map to the selected interface.

Syntax

`service-policy input *policy-map-name* [layer2]`

To remove the input policy map from the interface, use the `no service-policy input *policy-map-name* [layer2]` command.

Parameters

policy-map-name	Enter the name for the policy map in character format (16 characters maximum). You can identify an existing policy map or name one that does not yet exist.
layer2	(OPTIONAL) Enter the keyword `layer2` to specify a Layer 2 Class Map. The default is **Layer 3**.

Defaults

Layer 3

Command Modes

INTERFACE

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

You can attach a single policy-map to one or more interfaces to specify the service-policy for those interfaces. A policy map attached to an interface can be modified.

NOTE: The `service-policy` commands are not allowed on a port channel. The `service-policy input policy-map-name` command and the `service-class dynamic dot1p` command are not allowed simultaneously on an interface.

Related Commands	policy-map-input — creates an input policy map.

service-policy output

Apply an output policy map to the selected interface.

Syntax	`service-policy output` *`policy-map-name`* To remove the output policy map from the interface, use the `no service-policy output` *`policy-map-name`* command.

Parameters

policy-map-name	Enter the name for the policy map in character format (16 characters maximum). You can identify an existing policy map or name one that does not yet exist.

Defaults	none
Command Modes	INTERFACE

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information	A single policy-map can be attached to one or more interfaces to specify the service-policy for those interfaces. A policy map attached to an interface can be modified.
Related Commands	policy-map-output — creates an output policy map.

service-queue

Assign a class map and QoS policy to different queues.

Syntax	`service-queue` *`queue-id`* `[class-map` *`class-map-name`*`] [qos-policy` *`qos-policy-name`*`]` To remove the queue assignment, use the `no service-queue` *`queue-id`* `[class-map` *`class-map-name`*`] [qos-policy` *`qos-policy-name`*`]` command.

Parameters

queue-id	Enter the value used to identify a queue. The range is from 0 to 3 (four queues per interface; four queues are reserved for control traffic).
class-map *class-map-name*	(OPTIONAL) Enter the keyword `class-map` then the class map name assigned to the queue in character format (32 character maximum). NOTE: This option is available under `policy-map-input` only.
qos-policy *qos-policy-name*	(OPTIONAL) Enter the keywords `qos-policy` then the QoS policy name assigned to the queue in text format (32 characters maximum). This specifies the input QoS policy assigned to the queue under `policy-map-input` and output QoS policy under `policy-map-output` context.

Defaults none

Command Modes CONFIGURATION (conf-policy-map-in and conf-policy-map-out)

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information There are four queues per interface on the MXL switch. This command assigns a class map or QoS policy to different queues.

Related Commands service-policy output — applies an output policy map to the selected interface.

set

Mark outgoing traffic with a differentiated service code point (DSCP) or dot1p value.

Syntax `set {ip-dscp value | mac-dot1p value}`

Parameters

ip-dscp *value*	(OPTIONAL) Enter the keywords `ip-dscp` then the IP DSCP value. The range is from 0 to 63.
mac-dot1p *value*	Enter the keywords `mac-dot1p` then the dot1p value. The range is from 0 to 7.

Defaults none

Command Modes CONFIGURATION (conf-qos-policy-in)

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information After the IP DSCP bit is set, other QoS services can then operate on the bit settings.

show qos class-map

View the current class map information.

Syntax `show qos class-map [class-name]`

Parameters

class-name	(Optional) Enter the name of a configured class map.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show qos class-map

Class-map match-any CM
  Match ip access-group ACL
```

Related Commands class-map — identifies the class map.

show qos policy-map

View the QoS policy map information.

Syntax `show qos policy-map {summary [interface] | detail [interface]}`

Parameters

summary ***interface***	To view a policy map interface summary, enter the keyword `summary` and optionally one of the following keywords and slot/port or number information: • For a 40 Gigabit Ethernet interface, enter the keyword `FortyGigabitEthernet` then the slot/port information. • For a 10 Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.

detail *interface*	To view a policy map interface in detail, enter the keyword `detail` and optionally one of the following keywords and slot/port or number information: • For a 40 Gigabit Ethernet interface, enter the keyword `FortyGigabitEthernet` then the slot/port information. • For a 10 Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example (IPv4)

```
Dell#show qos policy-map detail tengigabitethernet 0/0

Interface tenGigabitEthernet 4/1

Policy-map-input policy
Trust diffserv
Queue# Class-map-name Qos-policy-name
 0       -             q0
 1       CM1           q1
 2       CM2           q2
 3       CM3           q3
```

Example (Summary IPv4)

```
Dell#sho qos policy-map summary

Interface policy-map-input policy-map-output
Gi 4/1     PM1                  -
Te 4/2     PM2         PMOut
Dell#
```

show qos policy-map-input

View the input QoS policy map details.

Syntax `show qos policy-map-input [policy-map-name] [class class-map-name] [qos-policy-input qos-policy-name]`

Parameters

policy-map-name	Enter the policy map name.

class *class-map-name*	Enter the keyword `class` then the class map name.
qos-policy-input *qos-policy-name*	Enter the keyword `qos-policy-input` then the QoS policy name.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show qos policy-map-input

Policy-map-input PolicyMapInput
Aggregate Qos-policy-name AggPolicyIn
Queue# Class-map-name  Qos-policy-name
0      ClassMap1       qosPolicyInput
Dell#
```

show qos policy-map-output

View the output QoS policy map details.

Syntax `show qos policy-map-output [policy-map-name] [qos-policy-output qos-policy-name]`

Parameters

policy-map-name	Enter the policy map name.
qos-policy-output *qos-policy-name*	Enter the keyword `qos-policy-output` then the QoS policy name.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show qos policy-map-output

Policy-map-output PolicyMapOutput
Aggregate Qos-policy-name AggPolicyOut
Queue#   Qos-policy-name
```

```
  0      qosPolicyOutput
Dell#
```

show qos qos-policy-input

View the input QoS policy details.

Syntax	`show qos qos-policy-input [`*`qos-policy-name`*`]`
Parameters	*qos-policy-name* Enter the QoS policy name.
Defaults	none
Command Modes	EXEC EXEC Privilege
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show qos qos-policy-input

Qos-policy-input QosInput
        Rate-police 100 50 peak 100 50
        Dscp 32
Dell#
```

show qos qos-policy-output

View the output QoS policy details.

Syntax	`show qos qos-policy-output [`*`qos-policy-name`*`]`
Parameters	*qos-policy-name* Enter the QoS policy name.
Defaults	none
Command Modes	EXEC EXEC Privilege
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show qos qos-policy-output

Qos-policy-output qmap_out
Bandwidth-percentage 10
Qos-policy-output qmap_wg
Rate-shape 100 50
Wred yellow wy
Wred green wg
Dell#
```

show qos statistics

View QoS statistics.

Syntax

```
show qos statistics {wred-profile [interface]} | [interface]
```

Parameters

wred-profile *interface*	Enter the keywords `wred-profile` and optionally one of the following keywords and slot/port or number information: • For a 40–Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a 10–Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
interface	Enter one of the following keywords and slot/port or number information: • For a 40–Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show qos statistics
Interface Te 0/20
Queue# Matched Pkts
0       0
1       0
2       0
3       0
Dell#
```

Usage Information

The following describes the `show qos statistics` command in the following example.

Field (ED and EE)	Description
Queue #	Queue Number
Matched Pkts	The number of packets that matched the class-map criteria. NOTE: When you configure `trust`, matched packet counters are not incremented in this field.

Example

```
Dell#show qos statistics wred-profile
Interface Te 0/20
Drop-statistic  Dropped Pkts
Green           0
Yellow          0
Out of Profile  0
Dell#
```

Usage Information

The following describes the `show qos statistics` command in the following example.

Field (EF)	Description
Queue #	Queue Number
Drop-statistic	Drop statistics for green, yellow, and out-of-profile packets.
Dropped Pkts	The total of the number of packets dropped for green, yellow and out-of-profile.

Related Commands

clear qos statistics — clears counters shown in `show qos statistics`.

show qos wred-profile

View the WRED profile details.

Syntax

`show qos wred-profile *wred-profile-name*`

Parameters

wred-profile-name	Enter the WRED profile name to view the profile details.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on THE MXL 10/40GbE Switch IO Module.

Example

```
Dell#show qos wred-profile

Wred-profile-name min-threshold max-threshold
wred_drop         0             0
wred_ge_y         1024          2048
wred_ge_g         2048          4096
wred_teng_y       4096          8192
wred_teng_g       8192          16384
WRED1             2000          7000
```

test cam-usage

Check the Input Policy Map configuration for the CAM usage.

Syntax

```
test cam-usage service-policy input policy-map stack-unit
{[number | [all]}
```

Parameters

policy-map	Enter the policy map name.
stack-unit *number*	(OPTIONAL) Enter the keywords `stack-unit` then the stack-unit number.
stack-unit all	(OPTIONAL) Enter the keywords `stack-unit all` all to indicate all the stack-units.

Defaults none

Command Modes EXEC

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

This feature allows you to determine if the CAM has enough space available before applying the configuration on an interface.

An input policy map with both Trust and Class-map configuration, the Class-map rules are ignored and only the Trust rule is programmed in the CAM. In such an instance, the Estimated CAM output column contains the size of the CAM space required for the Trust rule and not the Class-map rule.

The following describes the `text cam-usage service-policy input policy-map linecard` command shown in the following example.

Field	Description
stack-unit	Indicates the line card slot number.
Portpipe	Indicates the portpipe number.

Field	Description
CAM Partition	The CAM space where the rules are added.
Available CAM	Indicates the free CAM space, in the partition, for the classification rules. **NOTE:** The CAM entries reserved for the default rules are not included in the Available CAM column; free entries, from the default rules space, cannot be used as a policy map for the classification rules.
Estimated CAM per Port	Indicates the number of free CAM entries required (for the classification rules) to apply the input policy map on a single interface. **NOTE:** The CAM entries for the default rule are not included in this column; a CAM entry for the default rule is always dedicated to a port and is always available for that interface.
Status (Allowed ports)	Indicates if the input policy map configuration on an interface belonging to a linecard/port-pipe is successful — Allowed (n) — or not successful — Exception. The allowed number (n) indicates the number of ports in that port-pipe on which the Policy Map can be applied successfully.

NOTE: In a Layer 2 Policy Map, IPv4/IPv6 rules are not allowed; therefore, the output contains only L2ACL CAM partition entries.

Example

```
Dell# test cam-usage service-policy input pmap_l2 stack-unit
all

For a L2 Input Policy Map pmap_l2, the output must be as
follows,

Stack-unit|Portpipe|CAM Partition|Available CAM|Estimated CAM|
Status
        |        |             |             |per Port     |
(Allowed ports)
0           0          L2ACL       500          200
Allowed (2)
0           1          L2ACL       100          200
Exception
1           0          L2ACL       1000         200
Allowed (5)
1           1          L2ACL       0            200
Exception
                       …
                       …
                       …
13          1          L2ACL        400         200
Allowed (2)
Dell#
```

trust

Specify dynamic classification (DSCP) or dot1p to trust.

Syntax

```
trust {diffserv [fallback]| dot1p [fallback]}
```

Parameters

diffserv	Enter the keyword `diffserv` to specify trust of DSCP markings.
dot1p	Enter the keyword `dot1p` to specify trust dot1p configuration.
fallback	Enter the keyword `fallback` to classify packets according to their DSCP value as a secondary option in case no match occurs against the configured class maps.

Defaults

none

Command Modes

CONFIGURATION (conf-policy-map-in)

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

When you configure `trust`, matched bytes/packets counters are not incremented in the `show qos statistics` command.

Dynamic mapping honors packets marked according to the standard definitions of DSCP. The following lists the default mapping.

DSCP/CP hex Range (XXX)	DSCP Definition	Traditional IP Precedence	MXL Switch Internal Queue ID	DSCP/CP Decimal
111XXX		Network Control	3	48–63
110XXX		Internetwork Control	3	48–63
101XXX	EF (Expedited Forwarding)	CRITIC/ECP	2	32–47
100XXX	AF4 (Assured Forwarding)	Flash Override	2	32–47
011XXX	AF3	Flash	1	16–31
010XXX	AF2	Immediate	1	16–31
001XXX	AF1	Priority	0	0–15
000XXX	BE (Best Effort)	Best Effort	0	0–15

wred

Designate the WRED profile to yellow or green traffic.

Syntax

```
wred [[{yellow | green} profile-name] ecn]
```

To remove the WRED drop precedence, use the `no wred {yellow | green} [profile-name]` command.

Parameters

yellow | green	Enter the keyword `yellow` for yellow traffic. A DSCP value of xxx110 and xxx101 maps to yellow. Enter the keyword green for `green` traffic. A DSCP value of xxx0xx maps to green.
profile-name	Enter your WRED profile name in character format (16 character maximum). Or use one of the five pre-defined WRED profile names. Pre-defined Profiles: wred_drop, wred-ge_y, wred_ge_g, wred_teng_y, wred_teng_.
ecn	When you configure `wred ecn <cr>` command, instead of droppping the packets exponentially, Explicit Congestion Notification (ECN) marking is made on the packets.

Defaults

none

Command Modes

CONFIGURATION (conf-qos-policy-out)

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To assign drop precedence to green or yellow traffic, use this command. If there is no honoring enabled on the input, all the traffic defaults to green drop precedence.

Related Commands

wred-profile — creates a WRED profile and name that profile.

trust — defines the dynamic classification to trust DSCP.

wred ecn

To indicate network congestion, rather than dropping packets, use explicit congestion notification (ECN).

Syntax	`wred ecn` To stop marking packets, use the `no wred ecn` command.
Defaults	none
Command Modes	CONFIGURATION (conf-qos-policy-out)
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*. The following is a list of the Dell Networking OS version history for this command.

Version 9.0.2.0	Introduced on the S6000.
Version 8.3.19.0	Introduced on the S4820t.
Version 8.3.11.1	Introduced on the Z9000.
Version 8.3.7.0	Introduced on the S4810.

Usage Information

When you enable `wred ecn`, and the number of packets in the queue is below the minimum threshold, packets are transmitted per the usual WRED treatment.

When you enable `wred ecn`, and the number of packets in the queue is between the minimum threshold and the maximum threshold, one of the following two scenarios can occur:

- If the transmission endpoints are ECN-capable and traffic is congested, and the WRED algorithm determines that the packet should have been dropped based on the drop probability, the packet is transmitted and marked so the routers know the system is congested and can slow transmission rates.
- If neither endpoint is ECN-capable, the packet may be dropped based on the WRED drop probability. This behavior is the identical treatment that a packet receives when WRED is enabled without ECN configured on the router.

When you enable `wred ecn`, and the number of packets in the queue is above the maximum threshold, packets are dropped based on the drop probability. This behavior is the identical treatment a packet receives when WRED is enabled without ECN configured on the router.

Related Commands

wred-profile — creates a WRED profile and name that profile.

wred-profile

Create a WRED profile and name the profile.

Syntax	`wred-profile` *`wred-profile-name`* To remove an existing WRED profile, use the `no wred-profile` command.

Parameters

wred-profile-name	Enter your WRED profile name in character format (16 character maximum). Or use one of the pre-defined WRED profile names. You can configure up to 26 WRED profiles plus the five pre-defined profiles, for a total of 31 WRED profiles. Pre-defined Profiles: wred_drop, wred-ge_y, wred_ge_g, wred_teng_y, wred_teng_g.

Defaults	The five pre-defined WRED profiles. When you configure a new profile, the minimum and maximum threshold defaults to predefined wred_ge_g values.
Command Modes	CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information	Use the default pre-defined profiles or configure your own profile. You cannot delete the pre-defined profiles or their default values. This command enables WRED configuration mode — (conf-wred).

dscp

Sets the number of specific DSCP values for a color map profile to yellow or red.

Syntax	`dscp {yellow | red} [`*`list-dscp-values`*`]` To remove a color policy map profile, use the `no dscp {yellow | red} [`*`dscp-list`*`]` command.

Parameters

Yellow	Enter the `yellow` keyword. Traffic marked as yellow delivers traffic to the egress queue which either transmits the packet if it has available bandwidth or drops the packet due to no ability to send.

Red	Enter the `red` keyword. Traffic marked as red is dropped.
dscp-list	Enter a list of IP DSCP values. The *dscp-list* parameter specifies the full list of IP DSCP value(s) for the specified color. Each DSCP value in a list is separate values by commas – no spaces (1,2,3) or indicates a list of values separated by a hyphen (1-3). Range is `0` to `63`.

Defaults **None**

Command Modes CONFIG-COLOR-MAP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version 9.5.0.0	Introduced on the Z9000, S6000, S4820T, S4810, and MXL.

Usage Information

If the specified color-map does not exist, the Diffserv Manager (DSM) creates a color map and sets all the DSCP values to green (low drop precedence).

The default setting for each DSCP value (0-63) is green (low drop precedence). This command allows setting the number of specific DSCP values to yellow or red.

Important Points to Remember

- All DSCP values that are not specified as yellow or red are colored green.
- A DSCP value cannot be in both the yellow and red lists. Setting the red or yellow list with any DSCP value that is already in the other list results in an error and no update to that list is made.
- Each color map can only have one list of DSCP values for each color; any DSCP values previously listed for that color that are not in the new DSCP list are colored green.

Example

```
Dell(conf-dscp-color-map)# dscp yellow 9,10,11,13,15,16
```

Related Commands

qos dscp-color-map — configures the DSCP color map

qos dscp-color-policy— configures a DSCP color policy

qos dscp-color-map

Configure the DSCP color map.

Syntax	`qos dscp-color-map` *`map-name`* To remove a color map, use the no `qos dscp-color-map` *map-name* command.
Parameters	*map-name* — Enter the name of the DSCP color map. The map name can have a maximum of 32 characters.
Defaults	**None**
Command Modes	CONFIGURATION
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*. The following is a list of the Dell Networking OS version history for this command. Version 9.5.0.0 — Introduced on the Z9000, S6000, S4820T, S4810, and MXL.
Usage Information	A color map outlines the codepoint mappings to the appropriate color mapping (green, yellow, red) for the traffic. The system uses this information use to handle the traffic on the interface based on the traffic priority and places it into the appropriate shaping queue. You cannot delete a DSCP color map when it is configured on an interface. If you do, all the DSCP values are set to green (low drop precedence). To delete the DSCP color map that is being used by one or more interfaces, remove the DSCP map from each interface.
Example	`Dell(conf)#qos dscp-color-map mymap`
Related Commands	qos dscp-color-map— associates the DSCP color map profile with an interface so that all IP packets received on it is given a color based on that color map dscp— sets the number of specific DSCP values for color map profile to yellow or red.

qos dscp-color-policy

Associates the DSCP color map profile with an interface so that all IP packets received on it is given a color based on that color map.

Syntax	`dscp-color-policy` *`color-map-profile-name`* To remove a color policy map profile, use the no `dscp-color-policy` *`color-map-profile-name`* command.
Parameters	*color-map-profile-name* — Enter the color map profile name. The name can have a maximum of 32 characters.
Defaults	**None**
Command Modes	CONFIG-INTERFACE
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*. The following is a list of the Dell Networking OS version history for this command. Version 9.5.0.0 — Introduced on the Z9000, S6000, S4820T, S4810, and MXL.
Usage Information	If the specified color-map does not exist, the Diffserv Manager (DSM) creates a color map and sets all the DSCP values to green (low drop precedence).
Example	The following example assigns the color map, **bat-enclave-map**, to interface **te 0/11**.

```
Dell(conf)# int te 0/11
Dell(conf-if-te-0/11)# qos dscp-color-policy bat-enclave-map
```

Related Commands	dscp— sets the number of specific DSCP values for color map profile to yellow or red. qos dscp-color-map— configures the DSCP color map.

show qos dscp-color-policy

Display DSCP color policy configuration for one or all interfaces.

Syntax

```
show qos dscp-color-policy{summary [interface] | detail
{interface}}
```

Parameters

summary	Enter the `summary` keyword to display summary information about a color policy on one or more interfaces.
Detail	Enter the `detail` keyword to display detailed information about a color policy on one or more interfaces.
interface	Enter the name of the interface that has color policy configured.

Defaults **None**

Command Modes EXEC

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version 9.5.0.0	Introduced on the Z9000, S6000, S4820T, S4810, and MXL.

Example

```
Display summary information about a color policy on one or
more interfaces.

Dell# show qos dscp-color-policy summary

Interface     dscp-color-map
TE 0/10      mapONE
TE0/11       mapTWO

Display summary information about a color policy on a specific
interface.

Dell# show qos dscp-color-policy summary te 0/10
Interface    dscp-color-map
TE 0/10      mapONE

Displayed detailed color policy information on an interface.

Dell# show qos dscp-color-policy detail te 0/10
Interface TenGigabitEthernet 0/10

Dscp-color-map mapONE
  yellow 4,7
  red 20,30
```

Related Commands

— Displays DSCP color maps show qos dscp-color-map

show qos dscp-color-map

Display the DSCP color map for one or all interfaces.

Syntax	`show qos dscp-color-map` *`map-name`*
Parameters	*map-name* — Enter the name of the color map.
Defaults	**None**
Command Modes	EXEC
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*. The following is a list of the Dell Networking OS version history for this command. Version 9.5.0.0 — Introduced on the Z9000, S6000, S4820T, S4810, and MXL.
Related Commands	show qos dscp-color-policy — Displaying a DSCP Color Policy Configuration

Example

```
Display all DSCP color maps.

Dell# show qos dscp-color-map
Dscp-color-map mapONE
  yellow 4,7
  red 20,30
Dscp-color-map mapTWO
  yellow 16,55

Display a specific DSCP color map.

Dell# show qos dscp-color-map mapTWO
Dscp-color-map mapTWO
  yellow 16,55
```

44

Routing Information Protocol (RIP)

Routing information protocol (RIP) is a distance vector routing protocol. The Dell Networking Operating System (OS) supports both RIP version 1 (RIPv1) and RIP version 2 (RIPv2).

The implementation of RIP is based on IETF RFCs 2453 and RFC 1058. For more information about configuring RIP, refer to the *Dell Networking OS Configuration Guide*.

auto-summary

Restore the default behavior of automatic summarization of subnet routes into network routes. This command applies only to RIP version 2.

Syntax	`auto-summary` To send sub-prefix routing information, use the `no auto-summary` command.
Defaults	Enabled.
Command Modes	ROUTER RIP
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

clear ip rip

Update all the RIP routes in the routing table.

Syntax	`clear ip rip`
Command Modes	EXEC Privilege
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	This command triggers updates of the main RIP routing tables.

debug ip rip

Examine RIP routing information for troubleshooting.

Syntax

```
debug ip rip [interface | database | events [interface] |
packet [interface] | trigger]
```

To turn off debugging output, use the `no debug ip rip` command.

Parameters

interface	(OPTIONAL) Enter the interface type and ID as one of the following: • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.
database	(OPTIONAL) Enter the keyword `database` to display messages when there is a change to the RIP database.
events	(OPTIONAL) Enter the keyword `events` to debug only RIP protocol changes.
trigger	(OPTIONAL) Enter the keyword `trigger` to debug only RIP trigger extensions.

Command Modes

EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

default-information originate

Generate a default route for the RIP traffic.

Syntax

```
default-information originate [always] [metric metric-value]
[route-map map-name]
```

To return to the default values, use the `no default-information originate` command.

Parameters

always	(OPTIONAL) Enter the keyword `always` to enable the switch software to always advertise the default route.

metric *metric-value*	(OPTIONAL) Enter the keyword `metric` then a number as the metric value. The range is from 1 to 16. The default is **1**.
route-map *map-name*	(OPTIONAL) Enter the keywords `route-map` then the name of a configured route-map.

Defaults: Disabled. Metric: **1**.

Command Modes: ROUTER RIP

Command History:

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information: The default route must be present in the switch routing table for the `default-information originate` command to take effect.

default-metric

Change the default metric for routes. To ensure that all redistributed routes use the same metric value, use this command with the `redistribute` command.

Syntax: `default-metric` *`number`*

To return the default metric to the original values, use the `no default-metric` command.

Parameters:

number	Specify a number. The range is from 1 to 16. The default is **1**.

Defaults: **1**

Command Modes: ROUTER RIP

Command History:

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information: This command ensures that route information being redistributed is converted to the same metric value.

Related Commands: redistribute — allows you to redistribute routes learned by other methods.

description

Enter a description of the RIP routing protocol.

Syntax: `description {`*`description`*`}`

To remove the description, use the `no description {description}` command.

Parameters	
description	Enter a description to identify the RIP protocol (80 characters maximum).
Defaults	none
Command Modes	ROUTER RIP
Command History	**Version 8.3.16.1** — Introduced on the MXL 10/40GbE Switch IO Module..
Related Commands	router rip — enters ROUTER mode on the switch.

distance

Assign a weight (for prioritization) to all routes in the RIP routing table or to a specific route. Lower weights ("administrative distance") are preferred.

Syntax

```
distance weight [ip-address mask [prefix-name]]
```

To return to the default values, use the `no distance weight [ip-address mask]` command.

Parameters

weight	Enter a number from 1 to 255 for the weight (for prioritization). The default is **120**.
ip-address	(OPTIONAL) Enter the IP address, in dotted decimal format (A.B.C.D), of the host or network to receive the new distance metric.
mask	If you enter an IP address, also enter a mask for that IP address, in either dotted decimal format or /prefix format (/x).
prefix-name	(OPTIONAL) Enter a configured prefix list name.

Defaults	weight = **120**
Command Modes	ROUTER RIP
Command History	**Version 8.3.16.1** — Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	default-metric — assigns one distance metric to all routes learned using the `redistribute` command.

distribute-list in

Configure a filter for incoming routing updates.

Syntax

`distribute-list prefix-list-name in [interface]`

To delete the filter, use the `no distribute-list prefix-list-name in` command.

Parameters

prefix-list-name	Enter the name of a configured prefix list.
interface	(OPTIONAL) Identifies the interface type slot/port as one of the following: • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

Defaults Not configured.

Command Modes ROUTER RIP

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands ip prefix-list — enters PREFIX-LIST mode and configures a prefix list.

distribute-list out

Configure a filter for outgoing routing updates.

Syntax

`distribute-list prefix-list-name out [interface | bgp | connected | ospf | static]`

To delete the filter, use the `no distribute-list prefix-list-name out` command.

Parameters

prefix-list-name	Enter the name of a configured prefix list.
interface	(OPTIONAL) Identifies the interface type slot/port as one of the following:

- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

connected	(OPTIONAL) Enter the keyword `connected` to filter only directly connected routes.
ospf	(OPTIONAL) Enter the keyword `ospf` to filter all OSPF routes.
static	(OPTIONAL) Enter the keyword `static` to filter manually configured routes.

Defaults Not configured.

Command Modes ROUTER RIP

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands ip prefix-list — enters PREFIX-LIST mode and configures a prefix list.

ip poison-reverse

Set the prefix of the RIP routing updates to the RIP infinity value.

Syntax `ip poison-reverse`

To disable poison reverse, use the `no ip poison-reverse` command.

Defaults Disabled.

Command Modes INTERFACE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands ip split-horizon — sets the RIP routing updates to exclude routing prefixes.

ip rip receive version

To receive specific versions of RIP, set the interface. The RIP version you set on the interface overrides the version command in ROUTER RIP mode.

Syntax

```
ip rip receive version [1] [2]
```

To return to the default, use the `no ip rip receive version` command.

Parameters

1	(OPTIONAL) Enter the number `1` for RIP version 1.
2	(OPTIONAL) Enter the number `2` for RIP version 2.

Defaults **RIPv1** and **RIPv2**

Command Modes INTERFACE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information If you want the interface to receive both versions of RIP, use the `ip rip receive version 1 2` command.

Related Commands

ip rip send version — sets the RIP version for sending RIP traffic on an interface.

version — sets the RIP version the switch software uses.

ip rip send version

To send a specific version of RIP, set the interface. The version you set on the interface overrides the version command in ROUTER RIP mode.

Syntax

```
ip rip send version [1] [2]
```

To return to the default value, use the `no ip rip send version` command.

Parameters

1	(OPTIONAL) Enter the number `1` for RIP version 1. The default is RIPv1.
2	(OPTIONAL) Enter the number `2` for RIP version 2.

Defaults **RIPv1**

Command Modes INTERFACE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information	To enable the interface to send both version of RIP packets, use the `ip rip send version 1 2` command.
Related Commands	ip rip receive version — sets the RIP version for the interface to receive traffic. version — sets the RIP version for the switch software.

ip split-horizon

Enable split-horizon for RIP data on the interface. As described in RFC 2453, the split-horizon scheme prevents any routes learned over a specific interface to be sent back out that interface.

Syntax	`ip split-horizon` To disable split-horizon, use the `no ip split-horizon` command.
Defaults	Enabled
Command Modes	INTERFACE
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	ip poison-reverse — sets the prefix for RIP routing updates.

maximum-paths

Set RIP to forward packets over multiple paths.

Syntax	`maximum-paths` *`number`* To return to the default values, use the `no maximum-paths` commands.
Parameters	*number* Enter the number of paths. The range is from 1 to 16. The default is **4** paths.
Defaults	**4**
Command Modes	ROUTER RIP
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information	RIP supports a maximum of 16 ECMP paths.

neighbor

Define a neighbor router with which to exchange RIP information.

Syntax

`neighbor ip-address`

To delete a neighbor setting, use the `no neighbor ip-address` command.

Parameters

ip-address	Enter the IP address, in dotted decimal format, of a router with which to exchange information.

Defaults Not configured.

Command Modes ROUTER RIP

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

When a neighbor router is identified, unicast data exchanges occur. Multiple neighbor routers are possible.

To ensure that only specific interfaces are receiving and sending data, use the `passive-interface` command with the `neighbor` command.

Related Commands

passive-interface — sets the interface to only listen to RIP broadcasts.

network

Enable RIP for a specified network. To enable RIP on all networks connected to the switch, use this command.

Syntax

`network ip-address`

To disable RIP for a network, use the `no network ip-address` command.

Parameters

ip-address	Specify an IP network address in dotted decimal format. You cannot specify a subnet.

Defaults No RIP network is configured.

Command Modes	ROUTER RIP
Command History	Version 8.3.16.1 — Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	You can enable an unlimited number of RIP networks. RIP operates over interfaces configured with any address the `network` command specifies.

offset-list

Specify a number to add to the incoming or outgoing route metrics learned using RIP.

Syntax

`offset-list` *`prefix-list-name`* `{in | out}` *`offset`* `[`*`interface`*`]`

To delete an offset list, use the `no offset-list` *`prefix-list-name`* `{in | out}` *`offset`* `[`*`interface`*`]` command.

Parameters

prefix-list-name	Enter the name of an established Prefix list to determine which incoming routes are modified.
offset	Enter a number from zero (0) to 16 to be applied to the incoming route metric matching the access list specified. If you set an offset value to zero (0), no action is taken.
interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

Defaults	Not configured.
Command Modes	ROUTER RIP
Command History	Version 8.3.16.1 — Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	When the offset metric is applied to an interface, that value takes precedence over an offset value that is not extended to an interface.

Related Commands	ip prefix-list — enters PREFIX-LIST mode and configure a prefix list.

output-delay

Set the interpacket delay of successive packets to the same neighbor.

Syntax

`output-delay` *`delay`*

To return to the switch software defaults for interpacket delay, use the `no output-delay` command.

Parameters

delay	Specify a number of milliseconds as the delay interval. The range is from 8 to 50.

Defaults

Not configured.

Command Modes

ROUTER RIP

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

This command is intended for low-speed interfaces.

passive-interface

Suppress routing updates on a specified interface.

Syntax

`passive-interface` *`interface`*

To delete a passive interface, use the `no passive-interface` *`interface`* command.

Parameters

interface	Enter the following information: • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

Defaults	Not configured.
Command Modes	ROUTER RIP
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	Although the passive interface does not send or receive routing updates, the network on that interface still includes in RIP updates sent using other interfaces.
Related Commands	neighbor — enables RIP for a specified network. network — defines a neighbor.

redistribute

Redistribute information from other routing instances.

Syntax

`redistribute {connected | static}`

To disable redistribution, use the `no redistribute {connected | static}` command.

Parameters

connected	Enter the keyword `connected` to specify that information from active routes on interfaces is redistributed.
static	Enter the keyword `static` to specify that information from static routes is redistributed.

Defaults	Not configured.
Command Modes	ROUTER RIP
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	To redistribute the default route (0.0.0.0/0), configure the `default-information originate` command.
Related Commands	default-information originate — generates a default route for RIP traffic.

redistribute ospf

Redistribute routing information from an OSPF process.

Syntax

`redistribute ospf process-id [match external {1 | 2} | match internal | metric metric-value] [route-map map-name]`

To disable redistribution, use the `no redistribute ospf process-id [match external {1 | 2} | match internal | metric metric-value] [route-map map-name]` command.

Parameters

process-id	Enter a number that corresponds to the OSPF process ID to redistribute. The range is from 1 to 65355.
match external {1 | 2}	(OPTIONAL) Enter the keywords `match external` then the numbers `1` or `2` to indicated that external 1 routes or external 2 routes should be redistributed.
match internal	(OPTIONAL) Enter the keywords `match internal` to indicate that internal routes should be redistributed.
metric *metric-value*	(OPTIONAL) Enter the keyword `metric` then a number as the metric value. The range is from 0 to 16.
route-map *map-name*	(OPTIONAL) Enter the keywords `route-map` then the name of a configured route map.

Defaults Not configured.

Command Modes ROUTER RIP

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

router rip

To configure and enable RIP, enter ROUTER RIP mode.

Syntax

`router rip`

To disable RIP, use the `no router rip` command.

Defaults Disabled.

Command Modes CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information	To enable RIP, assign a network address using the `network` command.

Example

```
Dell(conf)#router rip
Dell(conf-router_rip)#
```

Related Commands	network — enables RIP.

show config

Display the changes you made to the RIP configuration. The default values are not shown.

Syntax	`show config`
Command Modes	ROUTER RIP
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell(conf-router_rip)#show config
!
router rip
  network 172.31.0.0
  passive-interface GigabitEthernet 0/1
Dell(conf-router_rip)#
```

show ip rip database

Display the routes that RIP learns. If the switch learned no RIP routes, no output is generated.

Syntax `show ip rip database [ip-address mask]`

Parameters

ip-address	(OPTIONAL) Specify an IP address in dotted decimal format to view RIP information on that network only. If you enter an IP address, also enter a mask for that IP address.
mask	(OPTIONAL) Specify a mask, in /network format, for the IP address.

Command Modes	EXEC Privilege
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show ip rip database` command shown in the following example.

Field	Description
Total number of routes in RIP database	Displays the number of RIP routes stored in the RIP database.
100.10.10.0/24 directly connected	Lists the routes directly connected.
150.100.0.0 redistributed	Lists the routes learned through redistribution.
209.9.16.0/24...	Lists the routes and the sources advertising those routes.

Example

```
Dell#show ip rip database
Total number of routes in RIP database: 1624
204.250.54.0/24
      [50/1] via 192.14.1.3, 00:00:12, GigabitEthernet 9/15
204.250.54.0/24     auto-summary
203.250.49.0/24
      [50/1] via 192.13.1.3, 00:00:12, GigabitEthernet 9/14
203.250.49.0/24     auto-summary
210.250.40.0/24
      [50/2] via 1.1.18.2, 00:00:14, Vlan 18
      [50/2] via 1.1.130.2, 00:00:12, Port-channel 30
210.250.40.0/24     auto-summary
207.250.53.0/24
      [50/2] via 1.1.120.2, 00:00:55, Port-channel 20
      [50/2] via 1.1.130.2, 00:00:12, Port-channel 30
      [50/2] via 1.1.10.2, 00:00:18, Vlan 10
207.250.53.0/24     auto-summary
208.250.42.0/24
      [50/2] via 1.1.120.2, 00:00:55, Port-channel 20
      [50/2] via 1.1.130.2, 00:00:12, Port-channel 30
      [50/2] via 1.1.10.2, 00:00:18, Vlan 10
208.250.42.0/24     auto-summary
```

show running-config rip

Display the current RIP configuration.

Syntax `show running-config rip`

Defaults none

Command Modes EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
show running-config rip
!
router rip
  distribute-list Test1 in
  distribute-list Test21 out
  network 10.0.0.0
  passive-interface GigabitEthernet 2/0
  neighbor 20.20.20.20
  redistribute ospf 999
  version 2
```

timers basic

Manipulate the RIP timers for routing updates, invalid, holddown times, and flush time.

Syntax

`timers basic update invalid holddown flush`

To return to the default settings, use the `no timers basic` command.

Parameters

update	Enter the number of seconds to specify the rate at which RIP routing updates are sent. The range is from zero (0) to 4294967295. The default is **30 seconds**.
invalid	Enter the number of seconds to specify the time interval before routing updates are declared invalid or expired. The invalid value should be at least three times the update timer value. The range is from zero (0) to 4294967295. The default is **180 seconds**.
holddown	Enter the number of seconds to specify a time interval during which the route is marked as unreachable but still sending RIP packets. The holddown value should be at least three times the update timer value. The range is from zero (0) to 4294967295. The default is **180 seconds**.
flush	Enter the number of seconds to specify the time interval during which the route is advertised as unreachable. When this interval expires, the route is flushed from the routing table. The flush value should be greater than the update value. The range is from zero (0) to 4294967295. The default is **240 seconds**.

Defaults

- update = **30 seconds**
- invalid = **180 seconds**
- holddown = **180 seconds**
- flush = **240 seconds**

Command Modes	ROUTER RIP
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	If you change the timers on one router, also synchronize the timers on all routers in the RIP domain.

version

Specify either RIP version 1 or RIP version 2.

Syntax	`version {1 | 2}` To return to the default version setting, use the `no version` command.
Parameters	**1** Enter the keyword `1` to specify RIP version 1. **2** Enter the keyword `2` to specify RIP version 2.
Defaults	The system sends RIPv1 and receives RIPv1 and RIPv2.
Command Modes	ROUTER RIP
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	ip rip receive version — sets the RIP version the interface receives. ip rip send version — sets the RIP version the interface sends.

45

Remote Monitoring (RMON)

The Dell Networking Operating System (OS) remote monitoring (RMON) is based on IEEE standards, providing both 32-bit and 64-bit monitoring and long-term statistics collection.

RMON supports the following RMON groups, as defined in RFC-2819, RFC-3273, RFC-3434 and RFC-4502:

- Ethernet Statistics Table; RFC-2819
- Ethernet Statistics High-Capacity Table; RFC-3273, 64bits
- Ethernet History Control Table; RFC-2819
- Ethernet History Table; RFC-2819
- Ethernet History High-Capacity Table; RFC-3273, 64bits
- Alarm Table; RFC-2819
- High-Capacity Alarm Table (64bits); RFC-3434, 64bits
- Event Table; RFC-2819
- Log Table; RFC-2819
- User History; RFC-4502
- Probe Configuration (Capabilities, SoftwareRev, HardwareRev, Date Time and ResetControl); RFC-4502

RMON does not support the following statistics:

- etherStatsCollisions
- etherHistoryCollisions
- etherHistoryUtilization

NOTE: Only simple network management protocol (SNMP) GET/GETNEXT access is supported. Configure RMON using the RMON commands. Collected data is lost during a chassis reboot.

rmon alarm

Set an alarm on any MIB object.

Syntax

```
rmon alarm number variable interval {delta | absolute} rising-threshold value event-number falling-threshold value event-number [owner string]
```

To disable the alarm, use the `no rmon alarm number` command.

Parameters

number	Enter the alarm integer number from 1 to 65535. The value must be unique in the RMON alarm table.

variable	Enter the MIB object to monitor. The variable must be in the SNMP OID format; for example, 1.3.6.1.2.1.1.3. The object type must be a 32-bit integer.
interval	Time, in seconds, the alarm monitors the MIB variables; this is the alarmSampleType in the RMON alarm table. The range is from 5 to 3600 seconds.
delta	Enter the keyword `delta` to test the change between MIB variables. This is the alarmSampleType in the RMON alarm table.
absolute	Enter the keyword `absolute` to test each MIB variable directly. This is the alarmSampleType in the RMON alarm table.
rising-threshold *value event-number*	Enter the keywords `rising-threshold` then the value (32 bit) the rising-threshold alarm is either triggered or reset. Then enter the event-number to trigger when the rising threshold exceeds its limit. This value is the same as the alarmRisingEventIndex or alarmTable of the RMON MIB. If there is no corresponding rising-threshold event, the value is zero.
falling-threshold *value event-number*	Enter the keywords `falling-threshold` then the value (32 bit) the falling-threshold alarm is either triggered or reset. Then enter the event-number to trigger when the falling threshold exceeds its limit. This value is the same as the alarmFallingEventIndex or the alarmTable of the RMON MIB. If there is no corresponding falling-threshold event, the value is zero.
owner *string*	(OPTIONAL) Enter the keyword `owner` then the owner name to specify an owner for the alarm. This is the alarmOwner object in the alarmTable of the RMON MIB.

Defaults **owner**

Command Modes CONFIGURATION

Command History		
	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

rmon collection history

Enable the RMON MIB history group of statistics collection on an interface.

Syntax

```
rmon collection history {controlEntry integer} [owner name]
[buckets number] [interval seconds]
```

To remove a specified RMON history group of statistics collection, use the `no rmon collection history {controlEntry integer}` command.

Parameters

controlEntry *integer*	Enter the keyword `controlEntry` to specify the RMON group of statistics using a value. Then enter an integer value from 1 to 65535 that identifies the RMON group of statistics. The integer value must be a unique index in the RMON history table.
owner *name*	(OPTIONAL) Enter the keyword `owner` then the owner name to record the owner of the RMON group of statistics.
buckets *number*	(OPTIONAL) Enter the keyword `buckets` then the number of buckets for the RMON collection history group of statistics. The bucket range is from 1 to 1000. The default is **50**.
interval *seconds*	(OPTIONAL) Enter the keyword `interval` then the number of seconds in each polling cycle. The range is from 5 to 3600 seconds. The default is **1800 seconds**.

Defaults none

Command Modes CONFIGURATION INTERFACE (config-if)

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

rmon collection statistics

Enable RMON MIB statistics collection on an interface.

Syntax `rmon collection statistics {controlEntry integer} [owner name]`

To remove RMON MIB statistics collection on an interface, use the `no rmon collection statistics {controlEntry integer}` command.

Parameters

controlEntry *integer*	Enter the keyword `controlEntry` to specify the RMON group of statistics using a value. Then enter an integer value from 1 to 65535 that identifies the RMON Statistic Table. The integer value must be a unique in the RMON statistic table.
owner *name*	(OPTIONAL) Enter the keyword `owner` then the owner name to record the owner of the RMON group of statistics.

Defaults none

Command Modes CONFIGURATION INTERFACE (config-if)

Command History	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

rmon event

Add an event in the RMON event table.

Syntax

```
rmon event number [log] [trap community] [description string]
[owner name]
```

To disable RMON on an interface, use the `no rmon event number` command.

Parameters

number	Assign an event number in integer format from 1 to 65535. The number value must be unique in the RMON event table.
log	(OPTIONAL) Enter the keyword `log` to generate an RMON log entry. The log entry is triggered and sets the eventType in the RMON MIB to log or log-and-trap. The default is **No log**.
trap *community*	(OPTIONAL) Enter the keyword `trap` then an SNMP community string to configure the eventType setting in the RMON MIB. This keyword sets either snmp-trap or log-and-trap. The default is **public**.
description *string*	(OPTIONAL) Enter the keyword `description` then a string describing the event.
owner *name*	(OPTIONAL) Enter the keyword `owner` then the name of the owner of this event.

Defaults As noted in the *Parameters* section.

Command Modes CONFIGURATION

Command History	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

rmon hc-alarm

Set an alarm on any MIB object.

Syntax

```
rmon hc-alarm number variable interval {delta | absolute}
rising-threshold value event-number falling-threshold value
event-number [owner string]
```

To disable the alarm, use the `no rmon hc-alarm number` command.

Parameters

number	Enter the alarm integer number from 1 to 65535. The value must be unique in the RMON alarm table.
variable	The MIB object to monitor. The variable must be in the SNMP OID format; for example, 1.3.6.1.2.1.1.3 The object type must be a 64-bit integer.
interval	Time, in seconds, the alarm monitors the MIB variables; this is the alarmSampleType in the RMON alarm table. The range is from 5 to 3600 seconds.
delta	Enter the keyword `delta` to test the change between MIB variables. This is the alarmSampleType in the RMON alarm table.
absolute	Enter the keyword `absolute` to test each MIB variable directly. This is the alarmSampleType in the RMON alarm table.
rising-threshold *value event-number*	Enter the keywords `rising-threshold` then the value (64 bit) the rising-threshold alarm is either triggered or reset. Then enter the event-number to trigger when the rising threshold exceeds its limit. This value is the same as the alarmRisingEventIndex or alarmTable of the RMON MIB. If there is no corresponding rising-threshold event, the value is zero.
falling-threshold *value event-number*	Enter the keywords `falling-threshold` then the value (64 bit) the falling-threshold alarm is either triggered or reset. Then enter the event-number to trigger when the falling threshold exceeds its limit. This value is the same as the alarmFallingEventIndex or the alarmTable of the RMON MIB. If there is no corresponding falling-threshold event, the value is zero.
owner *string*	(OPTIONAL) Enter the keyword `owner` then the owner name to specify an owner for the alarm. This is the alarmOwner object in the alarmTable of the RMON MIB.

Defaults **owner**

Command Modes CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

show rmon

Display the RMON running status including the memory usage.

Syntax	`show rmon`
Defaults	none
Command Modes	EXEC
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell# show rmon
RMON status
  total memory used 218840 bytes.
  ether statistics table: 8 entries, 4608 bytes
  ether history table: 8 entries, 6000 bytes
  alarm table: 390 entries, 102960 bytes
  high-capacity alarm table: 5 entries, 1680 bytes
  event table: 500 entries, 206000 bytes
  log table: 2 entries, 552 bytes
Dell#
```

show rmon alarms

Display the contents of the RMON alarm table.

Syntax `show rmon alarms [index] [brief]`

Parameters

index	(OPTIONAL) Enter the table index number to display just that entry.
brief	(OPTIONAL) Enter the keyword `brief` to display the RMON alarm table in an easy-to-read format.

Defaults	none
Command Modes	EXEC
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

Example (Index)

```
Dell#show rmon alarm 1
RMON alarm entry 1
  sample Interval: 5
  object: 1.3.6.1.2.1.1.3
  sample type: absolute value.
  value: 255161
  alarm type: rising or falling alarm.
  rising threshold: 1, RMON event index: 1
  falling threshold: 501, RMON event index: 501
  alarm owner: 1
  alarm status: OK
Dell#
```

Example (Brief)

```
Dell#show rmon alarm br
index   SNMP OID
--------------------------
1       1.3.6.1.2.1.1.3
2       1.3.6.1.2.1.1.3
3       1.3.6.1.2.1.1.3
4       1.3.6.1.2.1.1.3
5       1.3.6.1.2.1.1.3
6       1.3.6.1.2.1.1.3
7       1.3.6.1.2.1.1.3
8       1.3.6.1.2.1.1.3
9       1.3.6.1.2.1.1.3
10      1.3.6.1.2.1.1.3
11      1.3.6.1.2.1.1.3
12      1.3.6.1.2.1.1.3
13      1.3.6.1.2.1.1.3
14      1.3.6.1.2.1.1.3
15      1.3.6.1.2.1.1.3
16      1.3.6.1.2.1.1.3
17      1.3.6.1.2.1.1.3
18      1.3.6.1.2.1.1.3
19      1.3.6.1.2.1.1.3
20      1.3.6.1.2.1.1.3
21      1.3.6.1.2.1.1.3
22      1.3.6.1.2.1.1.3
Dell#
```

show rmon events

Display the contents of the RMON event table.

Syntax `show rmon events [index] [brief]`

Parameters

index	(OPTIONAL) Enter the table index number to display just that entry.
brief	(OPTIONAL) Enter the keyword `brief` to display the RMON event table in an easy-to-read format.

Defaults none

Command Modes EXEC

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example (Index)

```
Dell#show rmon event 1
RMON event entry 1
  description: 1
  event type: LOG and SNMP TRAP.
  event community: public
  event last time sent: none
  event owner: 1
  event status: OK
Dell#
```

Example (Brief)

```
Dell#show rmon event br
index    description
------------------------------
1        1
2        2
3        3
4        4
5        5
6        6
7        7
8        8
9        9
10       10
11       11
12       12
13       13
14       14
15       15
16       16
17       17
18       18
19       19
20       20
21       21
22       22
Dell#
```

show rmon hc-alarm

Display the contents of RMON High-Capacity alarm table.

Syntax

`show rmon hc-alarm [index] [brief]`

Parameters

index	(OPTIONAL) Enter the table index number to display just that entry.
brief	(OPTIONAL) Enter the keyword `brief` to display the RMON High-Capacity alarm table in an easy-to-read format.

Defaults

none

Command Modes

EXEC

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example (Index)

```
Dell#show rmon hc-alarm 1
RMON high-capacity alarm entry 1
  object: 1.3.6.1.2.1.1.3
  sample interval: 5
  sample type: absolute value.
  value: 185638
  alarm type: rising or falling alarm.
  alarm rising threshold value: positive.
  rising threshold: 1001, RMON event index: 1
  alarm falling threshold value: positive.
  falling threshold: 999, RMON event index: 6
  alarm sampling failed 0 times.
  alarm owner: 1
  alarm storage type: non-volatile.
  alarm status: OK
Dell#
```

Example (Brief)

```
Dell#show rmon hc-alarm brief
index     SNMP OID
----------------------------------
1         1.3.6.1.2.1.1.3
2         1.3.6.1.2.1.1.3
3         1.3.6.1.2.1.1.3
4         1.3.6.1.2.1.1.3
5         1.3.6.1.2.1.1.3
Dell#
```

show rmon history

Display the contents of the RMON Ethernet history table.

Syntax `show rmon history [`*`index`*`] [brief]`

Parameters

index	(OPTIONAL) Enter the table index number to display just that entry.
brief	(OPTIONAL) Enter the keyword `brief` to display the RMON Ethernet history table in an easy-to-read format

Defaults none

Command Modes EXEC

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example (Index)

```
Dell#show rmon history 6001
RMON history control entry 6001
  interface: ifIndex.100974631 GigabitEthernet 2/0
  bucket requested: 1
  bucket granted: 1
  sampling interval: 5 sec
  owner: 1
  status: OK
Dell#
```

Example (Brief)

```
Dell#show rmon history brief
index    ifIndex      interface
---------------------------------------
```

```
6001    100974631    GigabitEthernet 2/0
6002    100974631    GigabitEthernet 2/0
6003    101236775    GigabitEthernet 2/1
6004    101236775    GigabitEthernet 2/1
9001    134529054    GigabitEthernet 3/0
9002    134529054    GigabitEthernet 3/0
9003    134791198    GigabitEthernet 3/1
9004    134791198    GigabitEthernet 3/1
Dell#
```

show rmon log

Display the contents of the RMON log table.

Syntax

`show rmon log [index] [brief]`

Parameters

index	(OPTIONAL) Enter the table index number to display just that entry.
brief	(OPTIONAL) Enter the keyword `brief` to display the RMON log table in an easy-to-read format.

Defaults

none

Command Modes

EXEC

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The log table has a maximum of 500 entries. If the log exceeds that maximum, the oldest log entry is purged to allow room for the new entry.

Example (Index)

```
Dell#show rmon log 2
RMON log entry, alarm table index 2, log index 1
  log time: 14638 (THU AUG 12 22:10:40 2004)
  description: 2
Dell#
```

Example (Brief)

```
Dell#show rmon log br
eventIndex     description
------------------------------
2              2
4              4
Dell#
```

show rmon statistics

Display the contents of RMON Ethernet statistics table.

Syntax

`show rmon statistics [index] [brief]`

Parameters

index	(OPTIONAL) Enter the table index number to display just that entry.
brief	(OPTIONAL) Enter the keyword `brief` to display the RMON Ethernet statistics table in an easy-to-read format.

Defaults

none

Command Modes

EXEC

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example (Index)

```
Dell#show rmon statistics 6001
RMON statistics entry 6001
  interface: ifIndex.100974631 GigabitEthernet 2/0
  packets dropped: 0
  bytes received: 0
  packets received: 0
  broadcast packets: 0
  multicast packets: 0
  CRC error: 0
  under-size packets: 0
  over-size packets: 0
  fragment errors: 0
  jabber errors: 0
  collision: 0
  64bytes packets: 0
  65-127 bytes packets: 0
  128-255 bytes packets: 0
  256-511 bytes packets: 0
  512-1023 bytes packets: 0
  1024-1518 bytes packets: 0
  owner: 1
  status: OK
  <high-capacity data>
  HC packets received overflow: 0
  HC packets received: 0
  HC bytes received overflow: 0
  HC bytes received: 0
  HC 64bytes packets overflow: 0
  HC 64bytes packets: 0
  HC 65-127 bytes packets overflow: 0
  HC 65-127 bytes packets: 0
  HC 128-255 bytes packets overflow: 0
  HC 128-255 bytes packets: 0
  HC 256-511 bytes packets overflow: 0
  HC 256-511 bytes packets: 0
  HC 512-1023 bytes packets overflow: 0
  HC 512-1023 bytes packets: 0
  HC 1024-1518 bytes packets overflow: 0
  HC 1024-1518 bytes packets: 0
Dell#
```

Example (Brief)

```
Dell#show rmon statistics br
index    ifIndex    interface
----------------------------------------
6001    100974631    GigabitEthernet 2/0
6002    100974631    GigabitEthernet 2/0
6003    101236775    GigabitEthernet 2/1
6004    101236775    GigabitEthernet 2/1
9001    134529054    GigabitEthernet 3/0
9002    134529054    GigabitEthernet 3/0
9003    134791198    GigabitEthernet 3/1
9004    134791198    GigabitEthernet 3/1
Dell#
```

46

Rapid Spanning Tree Protocol (RSTP)

The Dell Networking Operating System (OS) implementation of rapid spanning tree protocol (RSTP) is based on the IEEE 802.1w standard spanning-tree protocol. The RSTP algorithm configures connectivity throughout a bridged local area network (LAN) that is comprised of LANs interconnected by bridges.

bridge-priority

Set the bridge priority for RSTP.

Syntax

`bridge-priority priority-value`

To return to the default value, use the `no bridge-priority` command.

Parameters

priority-value	Enter a number as the bridge priority value in increments of 4096. The range is from 0 to 61440. The default is **32768**.

Defaults

32768

Command Modes

CONFIGURATION RSTP (conf-rstp)

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

protocol spanning-tree rstp — enters rapid spanning tree mode.

debug spanning-tree rstp

Enable debugging of RSTP and view information on the protocol.

Syntax

```
debug spanning-tree rstp [all | bpdu interface {in | out} |
events]
```

To disable debugging, use the `no debug spanning-tree rstp` command.

Parameters

all	(OPTIONAL) Enter the keyword `all` to debug all spanning tree operations.

bpdu *interface* {in | out}	(OPTIONAL) Enter the keyword `bpdu` to debug the bridge protocol data units. (OPTIONAL) Enter the keyword `interface` along with the type slot/port of the interface you want displayed. Type slot/port options are the following: • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. Optionally, enter an in or out parameter with the optional interface: • For Receive, enter `in`. • For Transmit, enter `out`.
events	(OPTIONAL) Enter the keyword `events` to debug RSTP events.

Command Modes EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#debug spanning-tree rstp bpdu gigabitethernet 2/0 ?
in Receive (in)
out Transmit (out)
```

description

Enter a description of the rapid spanning tree.

Syntax `description {description}`

To remove the description, use the `no description {description}` command.

Parameters

description	Enter a description to identify the rapid spanning tree (80 characters maximum).

Defaults none

Command Modes	SPANNING TREE (The prompt is “config-rstp”.)
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	protocol spanning-tree rstp — enters SPANNING TREE mode on the switch.

disable

Disable RSTP globally on the system.

Syntax	`disable` To enable Rapid Spanning Tree Protocol, use the `no disable` command.
Defaults	RSTP is disabled.
Command Modes	CONFIGURATION RSTP (conf-rstp)
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	protocol spanning-tree rstp — enters SPANNING TREE mode on the switch.

forward-delay

Configure the amount of time the interface waits in the Listening State and the Learning State before transitioning to the Forwarding State.

Syntax	`forward-delay` *`seconds`* To return to the default setting, use the `no forward-delay` command.
Parameters	*seconds* Enter the number of seconds that the system waits before transitioning RSTP to the forwarding state. The range is from 4 to 30. The default is **15 seconds**.
Defaults	**15 seconds**
Command Modes	CONFIGURATION RSTP (conf-rstp)
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands	hello-time — changes the time interval between BPDUs. max-age — changes the wait time before RSTP refreshes the protocol configuration information.

hello-time

Set the time interval between the generation of the RSTP bridge protocol data units (BPDUs).

Syntax

`hello-time [milli-second] seconds`

To return to the default value, use the `no hello-time` command.

Parameters

seconds	Enter a number as the time interval between transmission of BPDUs. The range is from 1 to 10 seconds. The default is **2 seconds**.
milli-second	Enter the keywords `milli-second` to configure a hello time on the order of milliseconds. The range is from 50 to 950 milliseconds

Defaults

2 seconds

Command Modes

CONFIGURATION RSTP (conf-rstp)

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The hello time is encoded in BPDUs in increments of 1/256ths of a second. The standard minimum hello time in seconds is 1 second, which is encoded as 256. Millisecond hello times are encoded using values less than 256; the millisecond hello time equals (x/1000)*256.

When you configure millisecond hellos, the default hello interval of 2 seconds is still used for edge ports; the millisecond hello interval is not used.

Related Commands

forward-delay — changes the wait time before RSTP transitions to the Forwarding state.

max-age — changes the wait time before RSTP refreshes the protocol configuration information.

max-age

To maintain configuration information before refreshing that information, set the time interval for the RSTP bridge.

Syntax	`max-age seconds` To return to the default values, use the `no max-age` command.
Parameters	*max-age* — Enter a number of seconds that the waits before refreshing configuration information. The range is from 6 to 40 seconds. The default is **20 seconds**.
Defaults	**20 seconds**
Command Modes	CONFIGURATION RSTP (conf-rstp)
Command History	Version 8.3.16.1 — Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	forward-delay — changes the wait time before RSTP transitions to the Forwarding state. hello-time — changes the time interval between BPDUs.

edge-port bpdufilter default

To filter transmission of BPDU on port fast enabled interfaces, enable BPDU Filter globally.

Syntax	`edge-port bpdufilter default` To disable global bpdu filter default, use the `no edge-port bpdufilter default` command.
Parameters	*priority-value* — Enter a number as the bridge priority value in increments of 4096. The range is from 0 to 61440. The default is **32768**.
Defaults	Disabled
Command Modes	CONFIGURATION (conf-rstp)
Command History	Version 8.3.16.1 — Introduced on the MXL 10/40GbE Switch IO Module.

protocol spanning-tree rstp

To configure RSTP, enter RSTP mode.

Syntax	`protocol spanning-tree rstp` To exit RSTP mode, use the `exit` command.
Defaults	Not configured
Command Modes	CONFIGURATION
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	RSTP is not enabled when you enter RSTP mode. To enable RSTP globally on the system, use the `no disable` command from RSTP mode.

Example

```
Dell(conf)#protocol spanning-tree rstp
Dell(config-rstp)##no disable
```

Related Commands

disable — disables RSTP globally on the system.

show config

View the current configuration for the mode. Only non-default values are displayed.

Syntax	`show config`
Command Modes	CONFIGURATION RSTP (conf-rstp)
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell(conf-rstp)#show config
!
protocol spanning-tree rstp
  no disable
  bridge-priority 16384
```

spanning-tree rstp

Configure an RSTP interface with one of these settings: port cost, edge port with optional bridge port data unit (BPDU) guard, port priority, loop guard, or root guard.

Syntax	`spanning-tree rstp {cost port-cost | edge-port [bpduguard [shutdown-on-violation]] | bpdufilter | priority priority | {rootguard}}`

Parameters

cost *port-cost*	Enter the keyword `cost` then the port cost value. The range is from 1 to 200000. The defaults are: • 10-Gigabit Ethernet interface = **2000** • 40-Gigabit Ethernet interface = **1400** • Port Channel interface with one 10 Gigabit Ethernet = **2000** • Port Channel interface with one 40 Gigabit Ethernet = **1400** • Port Channel with two 10 Gigabit Ethernet = **1800** • Port Channel with two 40 Gigabit Ethernet = **600**
edge-port	Enter the keywords `edge-port` to configure the interface as a rapid spanning tree edge port.
bpduguard	(OPTIONAL) Enter the keyword `portfast` to enable Portfast to move the interface into Forwarding mode immediately after the root fails. Enter the keyword `bpduguard` to disable the port when it receives a BPDU.
shutdown-on-violation	(OPTIONAL) Enter the keywords `shutdown-on-violation` to hardware disable an interface when a BPDU is received and the port is disabled.
bpdufilter	(OPTIONAL) Enter the keyword `bpdufilter` to enable BPDU Filter to stop sending and receiving BPDUs on port enabled interfaces.
priority *priority*	Enter keyword `priority` then a value in increments of 16 as the priority. The range is from 0 to 240. The default is **128**.
rootguard	Enter the keyword `rootguard` to enable root guard on an RSTP port or port-channel interface.

Defaults	Not configured.
Command Modes	INTERFACE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The `BPDU guard` option prevents the port from participating in an active STP topology in case a BPDU appears on a port unintentionally, or is misconfigured, or is subject to a DOS attack. This option places the port into an Error Disable state if a BPDU appears and a message is logged so that the administrator can take corrective action.

> **NOTE:** A port configured as an edge port, on an RSTP switch, immediately transitions to the Forwarding state. Only configure ports connected to end-hosts as edge ports. Consider an edge port similar to a port with a `spanning-tree portfast` enabled.

If you do not enable `shutdown-on-violation`, BPDUs are still sent to the RPM CPU.

You cannot enable STP root guard and loop guard at the same time on a port. For example, if you configure loop guard on a port on which root guard is already configured, the following error message displays: `% Error: RootGuard is configured. Cannot configure LoopGuard`.

Enabling Portfast BPDU guard and loop guard at the same time on a port results in a port that remains in a Blocking state and prevents traffic from flowing through it. For example, when Portfast BPDU guard and loop guard are both configured:

- If a BPDU is received from a remote device, BPDU guard places the port in an Err-Disabled Blocking state and no traffic is forwarded on the port.
- If no BPDU is received from a remote device, loop guard places the port in a Loop-Inconsistent Blocking state and no traffic is forwarded on the port.

Example

```
Dell(conf)#interface gigabitethernet 4/0
Dell(conf-if-gi-4/0)#spanning-tree rstp edge-port
Dell(conf-if-gi-4/0)#show config
!
interface GigabitEthernet 4/0
  no ip address
  switchport
  spanning-tree rstp edge-port
  no shutdown
Dell#
```

spanning-tree rstp

Configure an RSTP interface with one of these settings: port cost, edge port with optional bridge port data unit (BPDU) guard, port priority, loop guard, or root guard.

Syntax

`spanning-tree rstp {cost` *`port-cost`* `| edge-port [bpduguard [shutdown-on-violation]] | bpdufilter | priority` *`priority`* `| {rootguard}}`

Parameters

cost *port-cost*	Enter the keyword `cost` then the port cost value. The range is from 1 to 200000. The defaults are:

- 10-Gigabit Ethernet interface = **2000**
- 40-Gigabit Ethernet interface = **1400**
- Port Channel interface with one 10 Gigabit Ethernet = **2000**
- Port Channel interface with one 40 Gigabit Ethernet = **1400**
- Port Channel with two 10 Gigabit Ethernet = **1800**
- Port Channel with two 40 Gigabit Ethernet = **600**

edge-port	Enter the keywords `edge-port` to configure the interface as a rapid spanning tree edge port.
bpduguard	(OPTIONAL) Enter the keyword `portfast` to enable Portfast to move the interface into Forwarding mode immediately after the root fails. Enter the keyword `bpduguard` to disable the port when it receives a BPDU.
shutdown-on-violation	(OPTIONAL) Enter the keywords `shutdown-on-violation` to hardware disable an interface when a BPDU is received and the port is disabled.
bpdufilter	(OPTIONAL) Enter the keyword `bpdufilter` to enable BPDU Filter to stop sending and receiving BPDUs on port enabled interfaces.
priority *priority*	Enter keyword `priority` then a value in increments of 16 as the priority. The range is from 0 to 240. The default is **128**.
rootguard	Enter the keyword `rootguard` to enable root guard on an RSTP port or port-channel interface.

Defaults

Not configured.

Command Modes

INTERFACE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The `BPDU guard` option prevents the port from participating in an active STP topology in case a BPDU appears on a port unintentionally, or is misconfigured, or is subject to a DOS attack. This option places the port into an Error Disable state if a BPDU appears and a message is logged so that the administrator can take corrective action.

NOTE: A port configured as an edge port, on an RSTP switch, immediately transitions to the Forwarding state. Only configure ports connected to end-hosts as edge ports. Consider an edge port similar to a port with a `spanning-tree portfast` enabled.

If you do not enable `shutdown-on-violation`, BPDUs are still sent to the RPM CPU.

You cannot enable STP root guard and loop guard at the same time on a port. For example, if you configure loop guard on a port on which root guard is already configured, the following error message displays: `% Error: RootGuard is configured. Cannot configure LoopGuard`.

Enabling Portfast BPDU guard and loop guard at the same time on a port results in a port that remains in a Blocking state and prevents traffic from flowing through it. For example, when Portfast BPDU guard and loop guard are both configured:

- If a BPDU is received from a remote device, BPDU guard places the port in an Err-Disabled Blocking state and no traffic is forwarded on the port.
- If no BPDU is received from a remote device, loop guard places the port in a Loop-Inconsistent Blocking state and no traffic is forwarded on the port.

Example

```
Dell(conf)#interface gigabitethernet 4/0
Dell(conf-if-gi-4/0)#spanning-tree rstp edge-port
Dell(conf-if-gi-4/0)#show config
!
interface GigabitEthernet 4/0
  no ip address
  switchport
  spanning-tree rstp edge-port
  no shutdown
Dell#
```

tc-flush-standard

Enable the MAC address flushing after receiving every topology change notification.

Syntax

`tc-flush-standard`

To disable, use the `no tc-flush-standard` command.

Defaults

Disabled

Command Modes

CONFIGURATION (conf-rstp)

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

By default, the system implements an optimized flush mechanism for RSTP. This implementation helps in flushing MAC addresses only when necessary (and less often), allowing for faster convergence during topology changes. However, if a standards-based flush mechanism is needed, you can turn on this *knob* command to enable flushing MAC addresses after receiving every topology change notification.

47

Security

This chapter contains various types of security commands offered in the Dell Networking Operating System (OS).

The commands are listed in the following sections:

- AAA Accounting Commands
- Authorization and Privilege Commands
- Authentication and Password Commands
- RADIUS Commands
- TACACS+ Commands
- SSH Server and SCP Commands
- Secure DHCP Commands

For configuration details, refer to the Security chapter in the *Dell Networking OS Configuration Guide*.

NOTE: Starting with the Dell Networking OS version 7.2.1.0, LEAP with MSCHAP v2 supplicant is implemented.

AAA Accounting Commands

AAA Accounting enables tracking of services that users are accessing and the amount of network resources being consumed by those services. When you enable AAA Accounting, the network server reports user activity to the TACACS+ security server in the form of accounting records. Each accounting record is comprised of accounting AV pairs and is stored on the access control server.

As with authentication and authorization, you must configure AAA Accounting by defining a named list of accounting methods, and then applying that list to various interfaces.

aaa accounting

Enable AAA Accounting and create a record for monitoring the accounting function.

Syntax

```
aaa accounting {system | exec | commands level role role-name}
{name | default}{start-stop | wait-start | stop-only} {tacacs+}
```

To disable AAA Accounting, use the `no aaa accounting {system | exec | command level} {name | default}{start-stop | wait-start | stop-only} {tacacs+}` command.

Parameters

system	Enter the keyword `system` to send accounting information of any other AAA configuration.
exec	Enter the keyword `exec` to send accounting information when a user has logged in to EXEC mode.
commands {*level*| role *role-name*}	Enter the keyword `command` then a privilege level for accounting of commands executed at that privilege level or enter the keyword `role` then the role name for accounting of commands executed by a user with that user role.
name | default	Enter one of the following: • For `name`, enter a user-defined name of a list of accounting methods. • For `default`, the default accounting methods used.
start-stop	Enter the keywords `start-stop` to send a "start accounting" notice at the beginning of the requested event and a "stop accounting" notice at the end of the event.
wait-start	Enter the keywords `wait-start` to ensure that the TACACS + security server acknowledges the start notice before granting the user's process request.
stop-only	Enter the keywords `stop-only` to instruct the TACACS+ security server to send a "stop record accounting" notice at the end of the requested user process.
tacacs+	Enter the keyword `tacacs+` to use TACACS+ data for accounting. The Dell Networking OS currently supports only TACACS+ accounting.

Defaults

none

Command Modes

CONFIGURATION

Command History

Version 9.5(0.0)	Introduced the support for roles on the MXL 10/40GbE Switch.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

In the example above, TACACS+ accounting is used to track all usage of EXEC command and commands on privilege level 15.

Privilege level 15 is the default. If you want to track usage at privilege level 1 for example, use the `aaa accounting command 1` command.

Example

```
Dell(conf)# aaa accounting exec default start-stop tacacs+
Dell(conf)# aaa accounting command 15 default start-stop tacacs
+
Dell(config)#
```

Related Commands	enable password — changes the password for the `enable` command. login authentication — enables AAA login authentication on the terminal lines. password — creates a password. tacacs-server host — specifies a TACACS+ server host.

aaa accounting suppress

Prevent the generation of accounting records of users with the user name value of NULL.

Syntax	`aaa accounting suppress null-username` To permit accounting records to users with user name value of NULL, use the `no aaa accounting suppress null-username` command.
Defaults	Accounting records are recorded for all users.
Command Modes	CONFIGURATION
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	The system issues accounting records for all users on the system, including users whose username string, due to protocol translation, is NULL. For example, a user who comes on line with the `aaa authentication login` *`method-list`* `none` command is applied. To prevent the accounting records from being generated for sessions that do not have user names associated to them, use the `aaa accounting suppress` command.

accounting

Apply an accounting method list to terminal lines.

Syntax

```
accounting {exec | commands {level | role role-name} method-list
```

Parameters

exec	Enter the keyword `exec` to apply an EXEC level accounting method list.
commands {*level*| role *role-name*}	Enter the keywords `commands level` to apply an EXEC and CONFIGURATION level accounting method list. Enter the keyword `role` and then the role name for accounting of commands executed by a user with that user role.

method-list	Enter a method list that you defined using the `aaa accounting exec` or `aaa accounting` commands.

Defaults none

Command Modes LINE

Command History

Version 9.5(0.0)	Introduced the support for roles on the MXL 10/40GbE Switch.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands aaa accounting — enables AAA Accounting and creates a record for monitoring the accounting function.

crypto key zeroize rsa

Removes the generated RSA host keys and zeroize the key storage location.

Syntax `crypto key zeroize rsa`

Defaults none

Command Modes CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide.*

The following is a list of the Dell Networking OS version history for this command.

Version 9.5(0.0)	Introduced on the Z9000, S6000, S4820T, S4810, MXL

Related Commands crypto key generate — Generate keys for SSH server

show accounting

Display the active accounting sessions for each online user.

Syntax `show accounting`

Defaults none

Command Modes	EXEC
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	This command steps through all active sessions and then displays the accounting records for the active account functions.

Example

```
Dell#show accounting
Active accounted actions on tty2, User guest Priv 1 Role <none>
  Task ID 1, EXEC Accounting record, 00:02:03
Elapsed,service=shell
Active accounted actions on tty3, User ad Priv 15 Role <none>
  Task ID 2, EXEC Accounting record, 00:01:22
Elapsed,service=shell
Active accounted actions on tty4, User ad Priv 15 Role <none>
  Task ID 11, EXEC Accounting record, 00:00:35 Elapsed,
service=shell
Active accounted actions on tty5, User ad Priv 1 Role sysadmin
  Task ID 16, EXEC Accounting record, 00:00:04 Elapsed,
service=shell
Dell#
```

Related Commands

aaa accounting — enables AAA Accounting and creates a record for monitoring the accounting function.

Authorization and Privilege Commands

To set command line authorization and privilege levels, use the following commands.

authorization

Apply an authorization method list to terminal lines.

Syntax

`authorization {exec | commands {level | role role-name} method-list`

Parameters

exec	Enter the keyword `exec` to apply an EXEC level accounting method list.
commands {*level* | role *role-name*}	Enter the keywords `commands` followed by either a privilege level for accounting of commands executed at that privilege level, or enter the keyword `role` then the role name for authorization of commands executed by a user with that user role.
method-list	Enter a method list that you defined using the `aaa accounting exec` or `aaa accounting` commands.

Defaults

none

Command Modes

LINE

Command History

Version 9.5(0.0)	Introduced the support for roles on the MXL 10/40GbE Switch.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

aaa authorization commands — sets the parameters that restrict (or permit) a user's access to EXEC and CONFIGURATION level commands

aaa authorization exec — sets the parameters that restrict (or permit) a user's access to EXEC level commands.

aaa authorization commands

Set parameters that restrict (or permit) a user's access to EXEC and CONFIGURATION level commands.

Syntax

```
aaa authorization commands {level | role role-name}{name | default} {local | tacacs+ | none}
```

Undo a configuration with the `no aaa authorization commands {level | role role-name}{name | default} {local | tacacs+ | none}` command.

Parameters

commands *level*	Enter the keyword `commands` then the command privilege level for command level authorization.
role *role-name*	Enter the keyword `role` then the role name.
name	Define a name for the list of authorization methods.
default	Define the default list of authorization methods.
local	Use the authorization parameters on the system to perform authorization.
tacacs+	Use the TACACS+ protocol to perform authorization.
none	Enter the keyword `none` to apply no authorization.

Defaults

none

Command Modes

CONFIGURATION

Command History

Version 9.5(0.0)	Introduced the support for roles on the MXL 10/40GbE Switch .

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

aaa authorization role-only

Configure authentication to use the user's role only when determining if access to commands is permitted.

Syntax

`aaa authorization role-only`

To return to the default setting, use the `no aaa authentication role-only` command.

Parameters

name	Enter a text string for the name of the user up to 63 characters. It cannot be one of the system defined roles (sysadmin, secadmin, netadmin, netoperator).
inherit *existing-role-name*	Enter the `inherit` keyword then specify the system defined role to inherit permissions from (sysadmin, secadmin, netadmin, netoperator).

Defaults

none

Command Modes

CONFIGURATION

Command History

Version 9.5.(0.0)	Introduced on the Z9000, S6000, S4820T, S4810, MXL

Usage Information

By default, access to commands are determined by the user's role (if defined) or by the user's privilege level. If the `aaa authorization role-only` command is enabled, then only the user's role is used.

Before you enable role-based only AAA authorization:

1. Locally define a system administrator user role.This will give you access to login with full permissions even if network connectivity to remote authentication servers is not available.
2. Configure login authentication on the console. This ensures that all users are properly identified through authentication no matter the access point
3. Specify an authentication method (RADIUS, TACACS+, or Local).
4. Specify authorization method (RADIUS, TACACS+ or Local).
5. Verify the configuration has been applied to the console or VTY line.

Related Commands	login authentication, password, radius-server host, tacacs-server host

aaa authorization config-commands

Set parameters that restrict (or permit) a user's access to EXEC level commands.

Syntax

```
aaa authorization config-commands
```

Disable authorization checking for CONFIGURATION level commands using the `no aaa authorization config-commands` command.

Defaults

Enabled when you configure `aaa authorization commands` command.

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

By default, the `aaa authorization commands` command configures the system to check both EXEC level and CONFIGURATION level commands. To enable only EXEC-level command checking, use the command `no aaa authorization config-commands`.

aaa authorization exec

Set parameters that restrict (or permit) a user's access to EXEC-level commands.

Syntax

```
aaa authorization exec {name | default} {local || tacacs+ ||
if-authenticated || none}
```

To disable authorization checking for EXEC level commands, use the `no aaa authorization exec` command.

Parameters

name	Define a name for the list of authorization methods.
default	Define the default list of authorization methods.
local	Use the authorization parameters on the system to perform authorization.
tacacs+	Use the TACACS+ protocol to perform authorization.
none	Enter the keyword `none` to apply no authorization.

Defaults

none

Command Modes	CONFIGURATION
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

privilege level (CONFIGURATION mode)

Change the access or privilege level of one or more commands.

Syntax

`privilege mode {level level command | reset command}`

To delete access to a level and command, use the `no privilege mode level level command` command.

Parameters

mode	Enter one of the following keywords as the mode for which you are controlling access: • `configure` for CONFIGURATION mode • `exec` for EXEC mode • `interface` for INTERFACE modes • `line` for LINE mode • `route-map` for ROUTE-MAP mode • `router` for ROUTER OSPF, ROUTER RIP, ROUTER ISIS and ROUTER BGP modes
level *level*	Enter the keyword `level` then a number for the access level. The range is from 0 to 15. Level 1 is EXEC mode and Level 15 allows access to all CLI modes and commands.
reset	Enter the keyword `reset` to return the security level to the default setting.
command	Enter the command's keywords to assign the command to a certain access level. You can enter one or all of the keywords.

Defaults	Not configured.
Command Modes	CONFIGURATION
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	To define a password for the level to which you are assigning privilege or access, use the `enable password` command.

privilege level (LINE mode)

Change the access level for users on the terminal lines.

Syntax

`privilege level level`

To delete access to a terminal line, use the `no privilege level level` command.

Parameters

level *level*	Enter the keyword `level` then a number for the access level. The range is from 0 to 15. Level 1 is EXEC mode and Level 15 allows access to all CLI modes.

Defaults

level = **15**

Command Modes

LINE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Authentication and Password Commands

To manage access to the system, use the following the commands.

aaa authentication enable

Configure AAA Authentication method lists for user access to EXEC privilege mode (the "Enable" access).

Syntax

`aaa authentication enable {default | method-list-name} method [... method2]`

To return to the default setting, use the `no aaa authentication enable {default | method-list-name} method [... method2]` command.

Parameters

default	Enter the keyword `default` then the authentication methods to use as the default sequence of methods for the Enable login. The default is `default enable`.
method-list-name	Enter a text string (up to 16 characters long) to name the list of enabled authentication methods activated at login.
method	Enter one of the following methods:

- `enable`: use the password the `enable password` command defines in CONFIGURATION mode.
- `line`: use the password the `password` command defines in LINE mode.
- `none`: no authentication.
- `radius`: use the RADIUS servers configured with the `radius-server host` command.
- `tacacs+`: use the TACACS+ server(s) configured with the `tacacs-server host` command.

... method2	(OPTIONAL) In the event of a "no response" from the first method, the system applies the next configured method.

Defaults

Use the `enable` password.

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

By default, the `Enable password` is used. If you configure `aaa authentication enable default`, the system uses the methods defined for `Enable access` instead.

Methods configured with the `aaa authentication enable` command are evaluated in the order they are configured. If authentication fails using the primary method, the system employs the second method (or third method, if necessary) automatically. For example, if the TACACS+ server is reachable, but the server key is invalid, the system proceeds to the next authentication method. The TACACS+ is incorrect, but the user is still authenticated by the secondary method.

Related Commands

enable password — changes the password for the `enable` command.

login authentication — enables AAA login authentication on the terminal lines.

password — creates a password.

radius-server host — specifies a RADIUS server host.

tacacs-server host — specifies a TACACS+ server host.

aaa authentication login

Configure AAA Authentication method lists for user access to EXEC mode (`Enable log-in`).

Syntax

```
aaa authentication login {method-list-name | default} method
[... method4]
```

To return to the default setting, use the `no aaa authentication login {`*`method-list-name`*` | default}` command.

Parameters

method-list-name	Enter a text string (up to 16 characters long) as the name of a user-configured method list that can be applied to different lines.
default	Enter the keyword `default` to specify that the method list specified is the default method for all terminal lines.
method	Enter one of the following methods: • `enable`: use the password the `enable password` command defines in CONFIGURATION mode. • `line`: use the password the `password` command defines in LINE mode. Not available if role-only is in use. • `none`: no authentication. Not available if role-only is in use. • `radius`: use the RADIUS servers configured with the `radius-server host` command. • `tacacs+`: use the TACACS+ servers configured with the `tacacs-server host` command.
... method4	(OPTIONAL) Enter up to four additional methods. In the event of a “no response” from the first method, the system applies the next configured method (up to four configured methods).

Defaults

Not configured (that is, no authentication is performed).

Command Modes

CONFIGURATION

Command History

Version 9.5(0.0)	Introduced the support for role on the MXL 10/40GbE Switch.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

By default, the locally configured username password is used. If you configure `aaa authentication login default`, the system uses the methods this command defines for login instead.

Methods configured with the `aaa authentication login` command are evaluated in the order they are configured. If users encounter an error with the first method listed, the Dell Networking OS applies the next method configured. If users fail the first method listed, no other methods are applied. The only exception is the local method. If the user’s name is not listed in the local database, the next method is applied. If the correct user name/password combination is not entered, the user is not allowed access to the switch.

NOTE: If authentication fails using the primary method, the system employs the second method (or third method, if necessary) automatically. For example, if the TACACS+ server is reachable, but the server key is invalid, the system proceeds to the next authentication method. The TACACS+ is incorrect, but the user is still authenticated by the secondary method.

After configuring the `aaa authentication login` command, configure the `login authentication` command to enable the authentication scheme on terminal lines.

Connections to the SSH server work with the following login mechanisms: local, radius, and tacacs.

Related Commands

login authentication — enables AAA login authentication on the terminal lines.

password — creates a password.

radius-server host — specifies a RADIUS server host.

tacacs-server host — specifies a TACACS+ server host.

access-class

Restrict incoming connections to a particular IP address in a defined IP access control list (ACL).

Syntax

`access-class` *`access-list-name`*

To delete a setting, use the `no access-class` command.

Parameters

access-list-name	Enter the name of an established IP Standard ACL.

Defaults

Not configured.

Command Modes

LINE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

line — applies an authentication method list to the designated terminal lines.

ip access-list standard — names (or selects) a standard access list to filter based on the IP address.

ip access-list extended — names (or selects) an extended access list based on the IP addresses or protocols.

enable password

Change the password for the `enable` command.

Syntax

`enable password [level level] [encryption-type] password`

To delete a password, use the `no enable password [encryption-type] password [level level]` command.

Parameters

level *level*	(OPTIONAL) Enter the keyword `level` then a number as the level of access. The range is from 1 to 15.
encryption-type	(OPTIONAL) Enter the number `7` or `0` as the encryption type. Enter a `7` then a text string as the hidden password. The text string must be a password that was already encrypted by a Dell Networking router. Use this parameter only with a password that you copied from the `show running-config` file of another Dell Networking router.
password	Enter a text string, up to 32 characters long, as the clear text password.

Defaults

No password is configured. *level* = **15**.

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To control access to command modes, use this command to define a password for a level and use the `privilege level (CONFIGURATION mode)` command.

Passwords must meet the following criteria:

- Start with a letter, not a number.
- Passwords can have a regular expression as the password. To create a password with a regular expression in it, use CNTL + v prior to entering regular expression. For example, to create the password `abcd]e`, you type “`abcd CNTL v ]e`”. When the password is created, you do not use the CNTL + v key combination and enter “`abcd]e`”.

NOTE: The question mark (?) and the tilde (~) are not supported characters.

Related Commands

show running-config — views the current configuration.

privilege level (CONFIGURATION mode) — controls access to the command modes within the switch.

enable restricted

Allows Dell Networking technical support to access restricted commands.

Syntax

`enable restricted [encryption-type] password`

To disallow access to restricted commands, use the `no enable restricted` command.

Parameters

encryption-type	(OPTIONAL) Enter the number `7` as the encryption type. Enter `7` followed a text string as the hidden password. The text string must be a password that was already encrypted by a Dell Networking router. Use this parameter only with a password that you copied from the `show running-config` file of another Dell Networking router.
password	Enter a text string, up to 32 characters long, as the clear text password.

Defaults

Not configured.

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Only Dell Networking Technical Support staff use this command.

enable secret

Change the password for the `enable` command.

Syntax

`enable secret [level level] [encryption-type] password`

To delete a password, use the `no enable secret [encryption-type] password [level level]` command.

Parameters

level *level*	(OPTIONAL) Enter the keyword `level` then a number as the level of access. The range is from 1 to 15.
encryption-type	(OPTIONAL) Enter the number `5` or `0` as the encryption type. Enter a `5` then a text string as the hidden password. The text string must be a password that was already encrypted by a Dell Networking router.

	Use this parameter only with a password that you copied from the `show running-config` file of another Dell Networking router.
password	Enter a text string, up to 32 characters long, as the clear text password.

Defaults No password is configured. *level* = **15**.

Command Modes CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information To control access to command modes, use this command to define a password for a level and use the `privilege level (CONFIGURATION mode)` command.

Passwords must meet the following criteria:

- Start with a letter, not a number.
- Passwords can have a regular expression as the password. To create a password with a regular expression in it, use CNTL + v prior to entering regular expression. For example, to create the password `abcd]e`, you type “`abcd CNTL v ]e`”. When the password is created, you do not use the CNTL + v key combination and enter “`abcd]e`”.

NOTE: The question mark (?) and the tilde (~) are not supported characters.

Related Commands show running-config — views the current configuration.

privilege level (CONFIGURATION mode) — controls access to the command modes within the switch.

login authentication

To designate the terminal lines, apply an authentication method list.

Syntax `login authentication {`*`method-list-name`*` | default}`

To use the local user/password database for login authentication, use the `no login authentication` command.

Parameters

method-list-name	Enter the keywords `method-list-name` to specify that method list, created in the `aaa authentication login` command, to be applied to the designated terminal line.
default	Enter the keyword `default` to specify that the default method list, created in the `aaa authentication login` command, is applied to the terminal line.

Defaults	No authentication is performed on the console lines. Local authentication is performed on the virtual terminal and auxiliary lines.
Command Modes	LINE
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	If you configure the `aaa authentication login default` command, the `login authentication default` command automatically is applied to all terminal lines.
Related Commands	aaa authentication login — selects the login authentication methods.

password

Specify a password for users on terminal lines.

Syntax

`password [encryption-type] password`

To delete a password, use the `no password password` command.

Parameters

encryption-type	(OPTIONAL) Enter either zero (`0`) or `7` as the encryption type for the password entered. The options are • `0` is the default and means the password is not encrypted and stored as clear text. • `7` means that the password is encrypted and hidden.
password	Enter a text string up to 32 characters long. The first character of the password must be a letter. You cannot use spaces in the password.

Defaults	No password is configured.
Command Modes	LINE
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	The system prompts users for these passwords when the method for authentication or authorization used is "line".
Related Commands	enable password — sets the password for the `enable` command. login authentication — configures an authentication method to log in to the switch. service password-encryption — encrypts all passwords configured in the system.

radius-server key — configures a key for all RADIUS communications between the switch and the RADIUS host server.

tacacs-server key — configures a key for communication between a TACACS+ server and client.

username — establishes an authentication system based on user names.

password-attributes

Configure the password attributes (strong password).

Syntax

```
password-attributes [min-length number] [max-retry number]
[lockout-period minutes][character-restriction [upper number]
[lower number] [numeric number] [special-char number]]
```

To return to the default, use the `no password-attributes [min-length number] [max-retry number] [lockout-period minutes] [character-restriction [upper number] [lower number] [numeric number] [special-char number]]` command.

Parameters

min-length *number*	(OPTIONAL) Enter the keywords `min-length` then the number of characters. The range is from 0 to 32 characters.
max-retry *number*	(OPTIONAL) Enter the keywords `max-retry` then the number of maximum password retries. The range is from 0 to 16.
lockout-period *minutes*	(OPTIONAL) Enter the keyword `lockout-period` then the number of minutes. The range is from `1` to `1440` minutes. The default is `0` minutes and the lockout-period is not enabled. This parameter enhances the security of the switch by locking out sessions on the Telnet or SSH sessions for which there has been a consecutive failed login attempts. The console is not locked out.
character-restriction	(OPTIONAL) Enter the keywords `character-restriction` to indicate a character restriction for the password.
upper *number*	(OPTIONAL) Enter the keyword `upper` then the upper number. The range is from 0 to 31.
lower *number*	(OPTIONAL) Enter the keyword `lower` then the lower number. The range is from 0 to 31.
numeric *number*	(OPTIONAL) Enter the keyword `numeric` then the numeric number. The range is from 0 to 31.
special-char *number*	(OPTIONAL) Enter the keywords `special-char` then the number of special characters permitted. The range is from 0 to 31.

Defaults	none
Command Modes	CONFIGURATION

Command History

Version 9.5(0.0)	Introduced the`lockout-period` option on the MXL 10/40GbE Switch.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

password — specifies a password for users on terminal lines.

service password-encryption

Encrypt all passwords configured in the system.

Syntax

`service password-encryption`

To store new passwords as clear text, use the `no service password-encryption` command.

Defaults	Enabled.
Command Modes	CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

CAUTION: Encrypting passwords with this command does not provide a high level of security. When the passwords are encrypted, you cannot return them to plain text unless you re-configure them. To remove an encrypted password, use the `no password password` command.

To keep unauthorized people from viewing passwords in the switch configuration file, use the `service password-encryption` command. This command encrypts the clear-text passwords created for user name passwords, authentication key passwords, the privileged command password, and console and virtual terminal line access passwords.

To view passwords, use the `show running-config` command.

show privilege

View your access level.

Syntax	`show privilege`
Command Modes	- EXEC - EXEC Privilege
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show privilege
Current privilege level is 15
Dell#
```

Related Commands: privilege level (CONFIGURATION mode) — assigns access control to different command modes.

show users

Allows you to view information on all users logged in to the switch.

Syntax

```
show users [all]
```

Parameters

all	(OPTIONAL) Enter the keyword `all` to view all terminal lines in the switch.

Command Modes: EXEC Privilege

Command History

Version 9.5(0.0)	Introduced the support for roles on the MXL 10/40GbE Switch.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information: The following describes the `show user` command shown in the following example.

Field	Description
(untitled)	Indicates with an asterisk (*) which terminal line you are using.
Line	Displays the terminal lines currently in use.
User	Displays the user name of all users logged in.
Host(s)	Displays the terminal line status.
Location	Displays the IP address of the user.

Example

```
Dell# show users
Authorization Mode:  role or privilege
    Line               User          Role              Priv
Host(s)    Location
*   0  console 0                     unassigned          1  idle
    2  vty 0           admin         unassigned          1
idle       10.16.127.35
    3  vty 1           ad            unassigned         15
idle       10.16.127.145
    4  vty 2           ad1           sysadmin            1
idle       10.16.127.141
    5  vty 3           ad1           sysadmin            1
idle       10.16.127.145
    6  vty 4           admin         unassigned          1
idle       10.16.127.141
    7  vty 5           ad            unassigned         15
idle       10.16.127.141
Dell#
```

Related Commands

username — enables a user.

timeout login response

Specify how long the software waits for the login input (for example, the user name and password) before timing out.

Syntax

`timeout login response` *`seconds`*

To return to the default values, use the `no timeout login response` command.

Parameters

seconds	Enter a number of seconds the software waits before logging you out. The range is: • VTY: the range is from 1 to 30 seconds, the default is **30 seconds**. • Console: the range is from 1 to 300 seconds, the default is **0 seconds** (no timeout). • AUX: the range is from 1 to 300 seconds, the default is **0 seconds** (no timeout).

Defaults

See the defaults settings shown in *Parameters*.

Command Modes

LINE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information	The software measures the period of inactivity defined in this command as the period between consecutive keystrokes. For example, if your password is "password" you can enter "p" and wait 29 seconds to enter the next letter.

username

Establish an authentication system based on user names.

Syntax

`username name [access-class access-list-name] [nopassword | {password | secret} [encryption-type] password] [privilege level] [role role-name]`

If you do not want a specific user to enter a password, use the `nopassword` option.

To delete authentication for a user, use the `no username name` command.

Parameters

name	Enter a text string for the name of the user up to 63 characters.
access-class *access-list-name*	Enter the keywords `access-class` then the name of a configured access control list (either an IP access control list or MAC access control list).
nopassword	Enter the keyword `nopassword` to specify that the user should not enter a password.
password	Enter the keyword `password` then the `encryption-type` or the password.
secret	Enter the keyword `secret` then the `encryption-type` or the password.
encryption-type	Enter an encryption type for the `password` that you enter. • `0` directs the system to store the password as clear text. It is the default encryption type when using the `password` option. • `7` to indicate that a password encrypted using a DES hashing algorithm follows. This encryption type is available with the `password` option only. • `5` to indicate that a password encrypted using an MD5 hashing algorithm follows. This encryption type is available with the `secret` option only, and is the default encryption type for this option.
password	Enter a string up to 32 characters long.
privilege *level*	Enter the keyword `privilege` then a number from zero (0) to 15.
role *role-name*	Enter the keyword `role` followed by the role name to associate with that user ID.

secret	Enter the keyword `secret` then the encryption type.

Defaults The default encryption type for the `password` option is **0**. The default encryption type for the `secret` option is **0**.

Command Modes CONFIGURATION

Command History

Version 9.5(0.0)	Introduced the support for roles on the MXL 10/40GbE Switch.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information To view the defined user names, use the `show running-config user` command.

Related Commands

password — specifies a password for users on terminal lines.

show running-config — views the current configuration.

RADIUS Commands

The following RADIUS commands are supported by Dell Networking operating system.

debug radius

View RADIUS transactions to assist with troubleshooting.

Syntax `debug radius`

To disable debugging of RADIUS, use the `no debug radius` command.

Defaults Disabled.

Command Modes EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

ip radius source-interface

Specify an interface’s IP address as the source IP address for RADIUS connections.

Syntax	`ip radius source-interface` *`interface`* To delete a source interface, use the `no ip radius source-interface` command.

Parameters

interface	Enter the following keywords and slot/port or number information: • For Loopback interfaces, enter the keyword `loopback` then a number from zero (0) to 16838. • For the Null interface, enter the keywords `null 0`. • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a ten-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

Defaults	Not configured.
Command Modes	CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

radius-server deadtime

Configure a time interval during which non-responsive RADIUS servers to authentication requests are skipped.

Syntax	`radius-server deadtime` *`seconds`* To disable this function or return to the default value, use the `no radius-server deadtime` command.

Parameters

seconds	Enter a number of seconds during which non-responsive RADIUS servers are skipped. The range is from 0 to 2147483647 seconds. The default is **0 seconds**.

Defaults	**0 seconds**

Command Modes	CONFIGURATION

Command History	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

radius-server host

Configure a RADIUS server host.

Syntax

```
radius-server host {hostname | ipv4-address} [auth-port port-number] [retransmit retries] [timeout seconds] [key [encryption-type] key]
```

Parameters

hostname	Enter the name of the RADIUS server host.
ipv4-address	Enter the IPv4 address (A.B.C.D) of the RADIUS server host.
auth-port *port-number*	(OPTIONAL) Enter the keywords `auth-port` then a number as the port number. The range is from zero (0) to 65535. The default port-number is **1812**.
retransmit *retries*	(OPTIONAL) Enter the keyword `retransmit` then a number as the number of attempts. This parameter overwrites the `radius-server retransmit` command. The range is from zero (0) to 100. The default is **3 attempts**.
timeout *seconds*	(OPTIONAL) Enter the keyword `timeout` then the seconds the time interval the switch waits for a reply from the RADIUS server. This parameter overwrites the `radius-server timeout` command. The range is from 0 to 1000. The default is **5 seconds**.
key [*encryption-type*] *key*	(OPTIONAL) Enter the keyword `key` then an optional encryption-type and a string up to 42 characters long as the authentication key. The RADIUS host server uses this authentication key and the RADIUS daemon operating on this switch. For the encryption-type, enter either zero (`0`) or `7` as the encryption type for the key entered. The options are: • `0` is the default and means the password is not encrypted and stored as clear text. • `7` means that the password is encrypted and hidden. Configure this parameter last because leading spaces are ignored.

Defaults	Not configured.
Command Modes	CONFIGURATION
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	To configure any number of RADIUS server hosts for each server host that is configured, use this command. The system searches for the RADIUS hosts in the order they are configured in the software. The global default values for the `timeout`, `retransmit`, and `key` optional parameters are applied, unless those values are specified in the `radius-server host` or other commands. To return to the global default values, if you configure the `timeout`, `retransmit`, or `key` values, include those keywords when using the `no radius-server host` command syntax.
Related Commands	login authentication — sets the database to be checked when a user logs in. radius-server key — sets an authentication key for RADIUS communications. radius-server retransmit — sets the number of times the RADIUS server attempts to send information. radius-server timeout — sets the time interval before the RADIUS server times out.

radius-server key

Configure a key for all RADIUS communications between the switch and the RADIUS host server.

Syntax

```
radius-server key [encryption-type] key
```

To delete a password, use the `no radius-server key` command.

Parameters

encryption-type	(OPTIONAL) Enter either zero (`0`) or `7` as the encryption type for the key entered. The options are: • `0` is the default and means the key is not encrypted and stored as clear text. • `7` means that the key is encrypted and hidden.
key	Enter a string that is the key to be exchanged between the switch and RADIUS servers. It can be up to 42 characters long.

Defaults Not configured.

Command Modes	CONFIGURATION
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	The key configured on the switch must match the key configured on the RADIUS server daemon. If you configure the `key` parameter in the `radius-server host` command, the key configured with the `radius-server key` command is the default key for all RADIUS communications.
Related Commands	radius-server host — configures a RADIUS host.

radius-server retransmit

Configure the number of times the switch attempts to connect with the configured RADIUS host server before declaring the RADIUS host server unreachable.

Syntax	`radius-server retransmit retries` To configure zero retransmit attempts, use the `no radius-server retransmit` command. To return to the default setting, use the `radius-server retransmit 3` command.
Parameters	*retries* Enter a number of attempts that the system tries to locate a RADIUS server. The range is from zero (0) to 100. The default is **3 retries**.
Defaults	**3 retries**
Command Modes	CONFIGURATION
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	radius-server host — configures a RADIUS host.

radius-server timeout

To reply to a request, configure the amount of time the RADIUS client (the switch) waits for a RADIUS host server .

Syntax

`radius-server timeout` *`seconds`*

To return to the default value, use the `no radius-server timeout` command.

Parameters

seconds	Enter the number of seconds between an unsuccessful attempt and the system times out. The range is from zero (0) to 1000 seconds. The default is **5 seconds**.

Defaults

5 seconds

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

radius-server host — configures a RADIUS host.

role

Changes command permissions for roles.

Syntax

`role mode` { { { `addrole` | `deleterole` } *role-name* } | `reset` } *command*

To delete access to a command, use the `no role` *mode* *`role-name`*

Parameters

mode	Enter one of the following keywords as the mode for which you are controlling access: configure for CONFIGURATION mode exec for EXEC mode interface for INTERFACE modes line for LINE mode route-map for Route-map mode router for Router mode

	addrole	Enter the keyword `addrole` to add permission to the command. You cannot add or delete rights for the sysadmin role.
	deleterole	Enter the keyword deleterole to remove access to the command. You cannot add or delete rights for the sysadmin role.
	role-name	Enter a text string for the name of the user role up to 63 characters. These are 3 system defined roles you can modify: secadmin, netadmin, and netoperator.
	reset	Enter the keyword `reset` to reset all roles back to default for that command.
	command	Enter the command's keywords to assign the command to a certain access level. You can enter one or more keywords.
Defaults	none	
Command Modes	CONFIGURATION	
Command History	Version 9.5.(0.0)	Introduced on the Z9000, S6000, S4820T, S4810, MXL
Related Commands	**userrole**	

TACACS+ Commands

The Dell Networking OS supports TACACS+ as an alternate method for login authentication.

debug tacacs+

To assist with troubleshooting, view TACACS+ transactions.

Syntax

```
debug tacacs+
```

To disable debugging of TACACS+, use the `no debug tacacs+` command.

Defaults: Disabled.

Command Modes: EXEC Privilege

Command History	**Version 8.3.16.1**	Introduced on the MXL 10/40GbE Switch IO Module.

ip tacacs source-interface

Specify an interface’s IP address as the source IP address for TACACS+ connections.

Syntax `ip tacacs source-interface` *`interface`*

To delete a source interface, use the `no ip tacacs source-interface` command.

Parameters

interface	Enter the following keywords and slot/port or number information: • For Loopback interfaces, enter the keyword `loopback` then a number from zero (0) to 16838. • For the Null interface, enter the keywords `null 0`. • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a ten-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

Defaults Not configured.

Command Modes CONFIGURATION

Command History	**Version 8.3.16.1**	Introduced on the MXL 10/40GbE Switch IO Module.

tacacs-server host

Specify a TACACS+ host.

Syntax `tacacs-server host {`*`hostname`*` | `*`ipv4-address`*`} [port `*`number`*`] [timeout `*`seconds`*`] [key `*`key`*`]`

Parameters

hostname	Enter the name of the TACACS+ server host.
ipv4-address	Enter the IPv4 address (A.B.C.D) of the TACACS+ server host.

port *number*	(OPTIONAL) Enter the keyword `port` then a number as the port to be used by the TACACS+ server. The range is from zero (0) to 65535. The default is **49**.
timeout *seconds*	(OPTIONAL) Enter the keyword `timeout` then the number of seconds the switch waits for a reply from the TACACS+ server. The range is from 0 to 1000. The default is **10 seconds**.
key *key*	(OPTIONAL) Enter the keyword `key` then a string up to 42 characters long as the authentication key. This authentication key must match the key specified in the `tacacs-server key` for the TACACS+ daemon.

Defaults Not configured.

Command Modes CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To list multiple TACACS+ servers to be used by the `aaa authentication login` command, configure this command multiple times.

If you are not configuring the switch as a TACACS+ server, you do not need to configure the `port`, `timeout` and `key` optional parameters. If you do not configure a key, the key assigned in the `tacacs-server key` command is used.

Related Commands

aaa authentication login — specifies the login authentication method.

tacacs-server key — configures a TACACS+ key for the TACACS server.

tacacs-server key

Configure a key for communication between a TACACS+ server and a client.

Syntax `tacacs-server key [`*`encryption-type`*`] key`

To delete a key, use the `no tacacs-server key` *`key`* command.

Parameters

encryption-type	(OPTIONAL) Enter either zero (`0`) or `7` as the encryption type for the key entered. The options are: • `0` is the default and means the key is not encrypted and stored as clear text. • `7` means that the key is encrypted and hidden.

key	Enter a text string, up to 42 characters long, as the clear text password. Leading spaces are ignored.

Defaults	Not configured.
Command Modes	CONFIGURATION
Command History	Version 8.3.16.1 — Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	The key configured with this command must match the key configured on the TACACS+ daemon.

SSH Server and SCP Commands

The Dell Networking OS supports secure shell (SSH) protocol versions 1.5 and 2.0. SSH is a protocol for secure remote login over an insecure network. SSH sessions are encrypted and use authentication.

crypto key generate

Generate keys for the SSH server.

Syntax
```
crypto key generate {rsa | rsa1}
```

Parameters

rsa	Enter the keyword `rsa` then the key size to generate a SSHv2 RSA host keys. The range is from 1024 to 2048 if you did not enable FIPS mode; if you enabled FIPS mode, you can only generate a 2048-bit key. The default is **1024**.
rsa1	Enter the keyword `rsa1` then the key size to generate a SSHv1 RSA host keys. The range is from 1024 to 2048. The default is **1024**.

Defaults	Key size **1024**; if you enable FIPS mode, the key size is **2048**.
Command Modes	CONFIGURATION
Command History	Version 8.3.16.1 — Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	The host keys are required for key-exchange by the SSH server. If the keys are not found when you enable the server (`ip ssh server enable`), the keys are automatically generated. This command requires user interaction and generates a prompt prior to overwriting any existing host keys.

NOTE: Only a user with superuser permissions should generate host-keys.

Example

```
Dell(conf)#crypto key generate rsa
Enter key size <1024-2048>. Default<1024>  :
Host key already exists. Overwrite (y/n)?y
Generating 1024-bit SSHv2 RSA key.
! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! !
 ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! !
Dell(conf)#
Dell(conf)#crypto key generate rsa1
Enter key size <1024-2048>. Default<1024>  :
Host key already exists. Overwrite (y/n)?y
Generating 1024-bit SSHv1 RSA key.
! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! !
 ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! !
Dell(conf)#
```

Related Commands

ip ssh server — enables the SSH server.

show crypto — displays the SSH host public keys.

debug ip ssh

Enables collecting SSH debug information.

Syntax

`debug ip ssh {client | server}`

To disable debugging, use the `no debug ip ssh {client | server}` command.

Parameters

client	Enter the keyword `client` to enable collecting debug information on the client.
server	Enter the keyword `server` to enable collecting debug information on the server.

Defaults

Disabled on both client and server.

Command Modes

EXEC

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Debug information includes details for key-exchange, authentication, and established session for each connection.

ip scp topdir

Identify a location for files used in secure copy transfer.

Syntax	`ip scp topdir directory` To return to the default setting, use the `no ip scp topdir` command.
Parameters	*directory* — Enter a directory name.
Defaults	The internal flash (`flash:`) is the default directory.
Command Modes	CONFIGURATION
Command History	Version 8.3.16.1 — Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	To configure the switch as an SCP server, use the `ip ssh server` command.
Related Commands	ip ssh server — enables the SSH and SCP server on the switch.

ip ssh authentication-retries

Configure the maximum number of attempts that should be used to authenticate a user.

Syntax	`ip ssh authentication-retries 1-10`
Parameters	*1-10* — Enter the number of maximum retries to authenticate a user. The range is from 1 to 10. The default is **3**.
Defaults	**3**
Command Modes	CONFIGURATION
Command History	Version 8.3.16.1 — Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	This command specifies the maximum number of attempts to authenticate a user on an SSH connection with the remote host for password authentication. SSH disconnects when the number of password failures exceeds authentication-retries.

ip ssh connection-rate-limit

Configure the maximum number of incoming SSH connections per minute.

Syntax `ip ssh connection-rate-limit 1-10`

Parameters

1-10	Enter the number of maximum numbers of incoming SSH connections allowed per minute. The range is from 1 to 10 per minute. The default is **10 per minute**.

Defaults **10 per minute**

Command Modes CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

ip ssh hostbased-authentication

Enable hostbased-authentication for the SSHv2 server.

Syntax `ip ssh hostbased-authentication enable`

To disable hostbased-authentication for SSHv2 server, use the `no ip ssh hostbased-authentication enable` command.

Parameters

enable	Enter the keyword `enable` to enable hostbased-authentication for SSHv2 server.

Defaults Disabled.

Command Modes CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information If you enable this command, clients can log in without a password prompt. This command provides two levels of authentication:

- rhost-authentication is done with the file specified in the `ip ssh rhostfile` command.
- checking client host-keys is done with the file specified in the `ip ssh pub-key-file` command.

NOTE: Administrators must specify the two files (`rhosts` and `pub-key-file`) to configure host-based authentication.

Related Commands	[ip ssh pub-key-file](#) — public keys of trusted hosts from a file. [ip ssh rhostsfile](#) — trusted hosts and users for rhost authentication.

ip ssh key-size

Configure the size of the server-generated RSA SSHv1 key.

Syntax	`ip ssh key-size 512-869`
Parameters	*512-869* — Enter the key-size number for the server-generated RSA SSHv1 key. The range is from 512 to 869. The default is **768**.
Defaults	Key size **768**
Command Modes	CONFIGURATION
Command History	Version 8.3.16.1 — Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	The server-generated key is used for SSHv1 key-exchange.

ip ssh password-authentication

Enable password authentication for the SSH server.

Syntax	`ip ssh password-authentication enable` To disable password-authentication, use the `no ip ssh password-authentication enable` command.
Parameters	enable — Enter the keyword `enable` to enable password-authentication for the SSH server.
Defaults	Enabled
Command Modes	CONFIGURATION
Command History	Version 8.3.16.1 — Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	With password authentication enabled, you can authenticate using the local, RADIUS, or TACACS+ password fallback order as configured.

ip ssh pub-key-file

Specify the file used for host-based authentication.

Syntax

`ip ssh pub-key-file {`*`WORD`*`}`

Parameters

WORD	Enter the file name for the host-based authentication.

Defaults

none

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

This command specifies the file used for the host-based authentication. The `creates/` file overwrites the `flash://ADMIN_DIR/ssh/knownhosts` file and deletes the user-specified file. Even though this command is a global configuration command, it does not appear in the running configuration because you only need to run this command once.

The file contains the OpenSSH-compatible public keys of the host for which host-based authentication is allowed. An example known host file format:

```
poclab4,123.12.1.123 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAox/
QQp8xYhzOxn07yh4VGPAoUfgKoieTHO9G4sNV+ui
+DWEc3cgYAcU5Lai1MU2ODrzhCwyDNp05tKBU3t
ReG1o8AxLi6+S4hyEMqHzkzBFNVqHzpQc
+Rs4p2urzV0F4pRKnaXdHf3Lk4D460HZRhhVrxqeNxPDpEn WIMPJi0ds=
ashwani@poclab4
```

NOTE: For `rhostfile` and `pub-key-file`, the administrator must FTP the file to the chassis.

Example

```
Dell#conf
Dell(conf)# ip ssh pub-key-file flash://knownhosts
Dell(conf)#
```

Related Commands

show ip ssh client-pub-keys — displays the client-public keys used for the host-based authentication.

ip ssh rekey

Configures the time rekey-interval or volume rekey-limit threshold at which to re-generate the SSH key during an SSH session.

Syntax

`ip ssh rekey [time rekey-interval] [volume rekey-limit]`

To reset to the default, use `no ip ssh rekey [time rekey-interval] [volume rekey-limit]` command.

Parameters

time *minutes*	Enter the keywords `time` then the amount of time in minutes. The range is from 10 to 1440 minutes. The default is **60** minutes
volume *rekey-limit*	Enter the keywords **volume** then the amount of volume in megabytes. The range is from 1 to 4096 to megabytes. The default is **1024 megabytes**

Defaults

The default time is **60** minutes. The default volume is **1024** megabytes.

Command Modes

CONFIGURATION mode

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version 9.5(0.0)	Introduced on the Z9000, S6000, S4820T, S4810, MXL

ip ssh rhostsfile

Specify the rhost file used for host-based authorization.

Syntax

`ip ssh rhostsfile {WORD}`

Parameters

WORD	Enter the rhost file name for the host-based authentication.

Defaults

none

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example	`Dell#conf`
	`Dell(conf)# ip ssh rhostsfile flash://shosts`
	`Dell(conf)#`

Usage Information	This command specifies the rhost file used for host-based authentication. This `creates/` file overwrites the `flash:/ADMIN_DIR/ssh/shosts` file and deletes the user-specified file. Even though this command is a global configuration command, it does not appear in the running configuration because you only need to run this command once. This file contains hostnames and usernames, for which hosts and users, rhost-authentication can be allowed. NOTE: For `rhostfile` and `pub-key-file`, the administrator must FTP the file to the switch.

ip ssh rsa-authentication (Config)

Enable RSA authentication for the SSHv2 server.

Syntax

```
ip ssh rsa-authentication enable
```

To disable RSA authentication, use the `no ip ssh rsa-authentication enable` command.

Parameters

enable	Enter the keyword `enable` to enable RSA authentication for the SSHv2 server.

Defaults Disabled.

Command Modes CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information Enabling RSA authentication allows the user to log in without being prompted for a password. In addition, the OpenSSH compatible SSHv2 RSA public key must be added to the list of authorized keys (`ip ssh rsa-authentication my-authorized-keys device://filename` command).

Related Commands ip ssh rsa-authentication (EXEC) — adds keys for RSA authentication.

ip ssh rsa-authentication (EXEC)

Add keys for the RSA authentication.

Syntax

`ip ssh rsa-authentication {my-authorized-keys WORD}`

To delete the authorized keys, use the `no ip ssh rsa-authentication {my-authorized-keys}` command.

Parameters

my-authorized-keys *WORD*	Enter the keywords `my-authorized-keys` then the filename of the RSA authorized-keys.

Defaults

none

Command Modes

EXEC

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

If you want to log in without being prompted for a password, log in through RSA authentication. To do that, first add the SSHv2 RSA public keys to the list of authorized keys. This command adds the specified RSA keys to the following file: `flash://ADMIN_DIR/ssh/authorized-keys-username` (where `username` is the user associated with this terminal).

NOTE: The `no` form of this command deletes the file `flash://ADMIN_DIR/ssh/ authorized-keys-username` file.

Related Commands

show ip ssh rsa-authentication — displays the RSA authorized keys.

ip ssh rsa-authentication (Config) — enables RSA authentication.

ip ssh server

Configure an SSH server.

Syntax

`ip ssh server {ciphers cipher-list} {enable | port port-number} [kex key-exchange-algorithm] [mac hmac-algorithm] [version {1 | 2}]`

To disable SSH server functions, use the `no ip ssh server {ciphers cipher-list} {enable | port port-number} {kex key-exchange-algorithm` command.

Parameters

enable	Enter the keyword `enable` to start the SSH server.

ciphers *cipher-list*	Enter the keyword `ciphers` and then a space-delimited list of ciphers that the SSH server supports. The following ciphers are available. • `3des-cbc` • `aes128-cbc` • `aes192-cbc` • `aes256-cbc` • `aes128-ctr` • `aes192-ctr` • `aes256-ctr` The default cipher list is used. • `3des-cbc` • `aes128-cbc` • `aes192-cbc` • `aes256-cbc` • `aes128-ctr` • `aes192-ctr` • `aes256-ctr`
mac *hmac-algorithm*	Enter the keyword `mac` then a space-delimited list of hash message authentication code (HMAC) algorithms supported by the SSH server for keying hashing for the message authentication. The following HMAC algorithms are available: • `hmac-sha1` • `hmac-sha1-96` • `hmac-sha2-256` • `hmac-sha2-256-96` When FIPS is enabled, the default HMAC algorithm is `hmac-sha1-96`. When FIPS is not enabled, the default HMAC algorithms are the following: • `hmac-md5` • `hmac-md5-96` • `hmac-sha1` • `hmac-sha1-96`

	• `hmac-sha2-256` • `hmac-sha2-256-96`
kex *key-exchange-algorithm*	Enter the keyword `kex` and then a space-delimited list of key exchange algorithms supported by the SSH server. The following key exchange algorithms are available: • `diffie-hellman-group-exchange-sha1` • `diffie-hellman-group1-sha1` • `diffie-hellman-group14-sha1` When FIPS is enabled, the default key-exchange-algorithm is `diffie-hellman-group14-sha1`. When FIPS is not enabled, the default key-exchange-algorithms are the following: • `diffie-hellman-group-exchange-sha1` • `diffie-hellman-group1-sha1,` • `diffie-hellman-group14-sha1`
port *port-number*	(OPTIONAL) Enter the keyword `port` then the port number of the listening port of the SSH server. The range is from 1 to 65535. The default is **22**.
[version {1 | 2}]	(OPTIONAL) Enter the keyword `version` then the SSH version 1 or 2 to specify only SSHv1 or SSHv2. NOTE: If you enable FIPS mode, you can only select version 2.

Defaults

Default listening port is **22**.

Command Modes

CONFIGURATION

Command History

Version 9.5(0.0)	Introduced the `cipher`, `kex` and `mac` options on the MXL 10/40GbE Switch.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

This command enables the SSH server and begins listening on a port. If a port is not specified, listening is on SSH default port 22.

NOTE: Starting with Dell Networking OS Release 9.2(0.0), SSH server is enabled by default.

Example

```
Dell# conf
Dell(conf)# ip ssh server port 45
Dell(conf)# ip ssh server enable
Dell#
```

Related Commands	show ip ssh — displays the ssh information.

show accounting

Display the active accounting sessions for each online user.

Syntax `show accounting`

Defaults none

Command Modes EXEC

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information This command steps through all active sessions and then displays the accounting records for the active account functions.

Example

```
Dell#show accounting
Active accounted actions on tty2, User guest Priv 1 Role <none>
  Task ID 1, EXEC Accounting record, 00:02:03
Elapsed,service=shell
Active accounted actions on tty3, User ad Priv 15 Role <none>
  Task ID 2, EXEC Accounting record, 00:01:22
Elapsed,service=shell
Active accounted actions on tty4, User ad Priv 15 Role <none>
  Task ID 11, EXEC Accounting record, 00:00:35 Elapsed,
service=shell
Active accounted actions on tty5, User ad Priv 1 Role sysadmin
  Task ID 16, EXEC Accounting record, 00:00:04 Elapsed,
service=shell
Dell#
```

Related Commands aaa accounting — enables AAA Accounting and creates a record for monitoring the accounting function.

show crypto

Display the public part of the SSH host-keys.

Syntax `show crypto key mypubkey {rsa | rsa1}`

Parameters

Key	Enter the keyword `key` to display the host public key.
mypubkey	Enter the keyword `mypubkey` to display the host public key.
rsa	Enter the keyword `rsa` to display the host SSHv2 RSA public key.

rsa1	Enter the keyword `rsa1` to display the host SSHv1 RSA public key.

Defaults

none

Command Modes

EXEC

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

This command is useful if the remote SSH client implements Strict Host Key Checking. You can copy the host key to your list of known hosts.

Example

```
Dell#show crypto key mypubkey rsa1
1024 65537
150477578329696762034442036788963493870885070479991994815292070
62670596651487238987338851388872
604558748599801007073218241492903069202754403378383368480816505
1718757388498171624789464677065606836272077
109398066281380715348265219018664838324451688712041531630245739
774449604335364302251481307373438756957374121

Dell#show crypto key mypubkey rsa
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgQC9IYgcUcc8wQm+5KUQgW/
zAs8V5STalGq4/+S+6H9axpQnA+A0xweeo5iR5hvPP6Vc+HS+
uWoQH+VOJ8H5Jxsm347XnYv/gpSqhgjZ/
C5UwFiucVkVfYu8RDcJVIuQhLvPEebIF5Q+sD8K89MXU90MAS/
UdoiJZSOIlbaCuSTW1Q==
Dell#
```

Related Commands

[crypto key generate](#) — generates the SSH keys.

show ip ssh

Display information about established SSH sessions.

Syntax

`show ip ssh`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show ip ssh
SSH server                : enabled.
SSH server version        : v1 and v2.
SSH server vrf            : default.
SSH server ciphers        : 3des-cbc,aes128-cbc,aes192-
cbc,aes256-cbc,aes128-ctr,aes192-ctr,aes256-ctr.
SSH server macs           : hmac-md5,hmac-md5-96,hmac-
sha1,hmac-sha1-96,hmac-sha2-256,hmac-sha2-256-96.
```

```
SSH server kex algorithms : diffie-hellman-group-exchange-
sha1,diffie-hellman-group1-sha1,diffie-hellman-group14-sha1.
Password Authentication   : enabled.
Hostbased Authentication  : disabled.
RSA       Authentication  : disabled.
   Vty          Encryption      HMAC            Remote IP
   2            aes128-cbc      hmac-md5        10.16.127.141
   4            aes128-cbc      hmac-md5        10.16.127.141
*  5            aes128-cbc      hmac-md5        10.16.127.141
Dell#
```

Related Commands

ip ssh server — configures an SSH server.

show ip ssh client-pub-keys — displays the client-public keys.

show ip ssh client-pub-keys

Display the client public keys used in host-based authentication.

Syntax

`show ip ssh client-pub-keys`

Defaults

none

Command Modes

EXEC

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

This command displays the contents of the `flash://ADMIN_DIRssh/knownhosts` file.

Example

```
Dell# show ip ssh client-pub-keys
4.8.1.2 ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAu5NoTbmnLxBknaeXZmUJMupNwNUoGlo1/
yLPI5eehQTyaldRPHtGyPlcmMbCH+QJkqtyiw
DPmH4njyDMYDCXY85vc55ibWsN9qalagklnh2cj2q4nYj5x8+8OOhYeFPaHiygd
8U/FXict61jWs84Co1UTsAgRzDJ9aUSS75TVac
= root@dt-maa-linux-1.force10networks.com
2200:2200:2200:2200:2200::2202 ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAu5NoTbmnLxBknaeXZmUJMupNwNUoGlo1/
yLPI5eehQTyaldR
PHtGyPlcmMbCH
+QJkqtyiwDPmH4njyDMYDCXY85vc55ibWsN9qalagklnh2cj2q4nYj5x8+8OOhY
eFPaHiygd8U/FXict61jWs84Co1UTsAgRzDJ9a
USS75TVac= root@dt-maa-linux-1.force10networks.com
10.16.151.48 ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAu5NoTbmnLxBknaeXZmUJMupNwNUoGlo1/
yLPI5eehQTyaldRPHtGyPlcmMbCH+QJ
kqtyiwDPmH4njyDMYDCXY85vc55ibWsN9qalagklnh2cj2q4nYj5x8+8OOhYeFP
aHiygd8U/FXict61jWs84Co1UTsAgRzDJ9aUSS75TVac=
Dell#
```

Related Commands

ip ssh pub-key-file — configures the filename for the host-based authentication.

show ip ssh rsa-authentication

Display the authorized-keys for the RSA authentication.

Syntax `show ip ssh rsa-authentication {my-authorized-keys}`

Parameters

my-authorized-keys	Display the RSA authorized keys.

Defaults none

Command Modes EXEC

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information This command displays the contents of the `flash:/ADMIN_DIR/ssh/authorized-keys.username` file.

Example

```
Dell#show ip ssh rsa-authentication my-authorized-keys
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAyB17l4gFp4r2DRHIvMc1VZd0Sg5GQxRV1y1
X1JOMeO6Nd0WuYyzrQMM
4qJAoBwtneOXfLBcHF3V2hcMIqaZN+CRCnw/
zCMlnCf0+qVTd1oofsea5r09kS0xTp0CNfHXZ3NuGCq9Ov33m9+U9tMwhS8vy8A
VxdH4x4km3c3t5Jvc=
freedom@poclab4

Dell#
```

Related Commands Xip ssh rsa-authentication (Config) — configures the RSA authorized keys.

show role

Display information on permissions assigned to a command, including user role and/or permission level.

Syntax `show role mode {`*`mode`*`} {`*`command`*`}`

Parameters

command	Enter the command's keywords to assign the command to a certain access level. You can enter one or all of the keywords.
mode *mode*	Enter keyword then one of the following modes. • configure • exec

- interface
- line
- route-map
- router

Defaults	none
Command Modes	EXEC Privilege

Command History

Version 9.5(0.0)	Introduced on the Z9000, S6000, S4820T, S4810, MXL

Examples

```
Dell#show role mode configure username
Role access: sysadmin

Dell#show role mode configure management route
Role access: netadmin, sysadmin

Dell#show role mode configure management crypto-policy
Role access: secadmin, sysadmin
```

Related Commands userrole, username, privilege

show users

Allows you to view information on all users logged in to the switch.

Syntax `show users [all]`

Parameters

all	(OPTIONAL) Enter the keyword `all` to view all terminal lines in the switch.

Command Modes EXEC Privilege

Command History

Version 9.5(0.0)	Introduced the support for roles on the MXL 10/40GbE Switch.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show user` command shown in the following example.

Field	Description
(untitled)	Indicates with an asterisk (*) which terminal line you are using.

Field	Description
Line	Displays the terminal lines currently in use.
User	Displays the user name of all users logged in.
Host(s)	Displays the terminal line status.
Location	Displays the IP address of the user.

Example

```
Dell# show users
Authorization Mode:  role or privilege
    Line                 User         Role              Priv
Host(s)     Location
*    0  console 0                     unassigned         1  idle
     2  vty 0            admin        unassigned         1
idle        10.16.127.35
     3  vty 1            ad           unassigned        15
idle        10.16.127.145
     4  vty 2            ad1          sysadmin           1
idle        10.16.127.141
     5  vty 3            ad1          sysadmin           1
idle        10.16.127.145
     6  vty 4            admin        unassigned         1
idle        10.16.127.141
     7  vty 5            ad           unassigned        15
idle        10.16.127.141
Dell#
```

Related Commands

username — enables a user.

show userroles

Display information on all defined user roles.

Syntax

```
show userroles
```

Example

```
Dell#show userroles
Role           Inheritance  Modes
netoperator                 Exec
netadmin                    Exec Config Interface Line Router IP
                            Route-map Protocol MAC
secadmin                    Exec Config
sysadmin                    Exec Config Interface Line Router IP
                            Route-map Protocol MAC
netoperator
testadmin      netadmin     Exec Config Interface Line Router IP
                            Route-map Protocol MAC
```

Command Modes

EXEC Privilege

Command History	**Version 9.5(0.0)**	Introduced on the Z9000, S6000, S4820T, S4810, MXL.

Related Commands: userrole, username

ssh

Open an SSH connection specifying the host name, username, port number and version of the SSH client.

Syntax

```
ssh {hostname | ipv4 address} [-l username | -p port-number | -
v {1 | 2}]
```

Parameters

hostname	(OPTIONAL) Enter the IP address or the host name of the remote device.
ipv4 address	(OPTIONAL) Enter the IP address in dotted decimal format A.B.C.D.
-l *username*	(OPTIONAL) Enter the keyword `-l` then the user name used in this SSH session. The default is the user name of the user associated with the terminal.
-p *port-number*	(OPTIONAL) Enter the keyword `-p` then the port number. The range is from 1 to 65536. The default is **22**.
-v {1 | 2}	(OPTIONAL) Enter the keyword `-v` then the SSH version 1 or 2. The default is the version from the protocol negotiation.

Defaults: As shown in the *Parameters* section.

Command Modes: EXEC Privilege

Command History	**Version 8.3.16.1**	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information: The system supports both inbound and outbound SSH sessions using IPv4 or IPv6 addressing. Inbound SSH supports accessing the system through the management interface as well as through a physical Layer 3 interface.

Example

```
Dell#ssh 10.16.151.48 -l anvltest

Trying 10.16.151.48...
01:18:16: %STKUNIT0-M:CP %SEC-5-SSH_USAGE: Initiated SSH
Client v2 (FIPS Disabled) to anvltest@10.16.151.48 by default
from console
anvltest@10.16.151.48's password:
Last login: Thu Jan  5 00:17:47 2012 from login-maa-101
[anvltest@dt-maa-linux-1 ~]# exit
```

```
logout
Dell#
```

Secure DHCP Commands

The dynamic host configuration protocol (DHCP) as defined by RFC 2131 provides no authentication or security mechanisms. Secure DHCP is a suite of features that protects networks that use dynamic address allocation from spoofing and attacks.

clear ip dhcp snooping

Clear the DHCP binding table.

Syntax	`clear ip dhcp snooping binding`
Defaults	none
Command Modes	EXEC Privilege
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	show ip dhcp snooping — displays the contents of the DHCP binding table.

ip dhcp relay

Enable Option 82.

Syntax	`ip dhcp relay information-option [trust-downstream]`
Parameters	**trust-downstream** Configure the system to trust Option 82 when it is received from the previous-hop router.
Defaults	Disabled.
Command Modes	CONFIGURATION
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

ip dhcp snooping

Enable DHCP Snooping globally.

Syntax	`[no] ip dhcp snooping`
Defaults	Disabled.
Command Modes	CONFIGURATION
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	When enabled, no learning takes place until you enable snooping on a VLAN. After disabling DHCP Snooping, the binding table is deleted and Option 82, IP Source Guard, and Dynamic ARP Inspection are disabled.
Related Commands	ip dhcp snooping vlan — enables DHCP Snooping on one or more VLANs.

ip dhcp snooping database

Delay writing the binding table for a specified time.

Syntax	`ip dhcp snooping database write-delay` *`minutes`*
Parameters	*minutes* The range is from 5 to 21600.
Defaults	none
Command Modes	CONFIGURATION
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

ip dhcp snooping binding

Create a static entry in the DHCP binding table.

Syntax	`[no] ip dhcp snooping binding mac` *`address`* `vlan-id` *`vlan-id`* `ip` *`ip-address`* `interface` *`type slot/port`* `lease` *`number`*
Parameters	mac *address* Enter the keyword `mac` then the MAC address of the host to which the server is leasing the IP address.

vlan-id *vlan-id*	Enter the keywords `vlan-id` then the VLAN to which the host belongs. The range is from 2 to 4094.
ip *ip-address*	Enter the keyword `ip` then the IP address that the server is leasing.
interface *type*	Enter the keyword `interface` then the type of interface to which the host is connected. • For a ten-Gigabit Ethernet interface, enter the keyword `tengigabitethernet`. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE`.
slot/port	Enter the slot and port number of the interface.
lease *time*	Enter the keyword `lease` then the amount of time the IP address is leased. The range is from 1 to 4294967295.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands show ip dhcp snooping — displays the contents of the DHCP binding table.

ip dhcp snooping database renew

Renew the binding table.

Syntax `ip dhcp snooping database renew`

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.19.0	Introduced on the MXL 10/40GbE Switch IO Module.

ip dhcp snooping trust

Configure an interface as trusted.

Syntax	`[no] ip dhcp snooping trust`
Defaults	Untrusted
Command Modes	INTERFACE
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

ip dhcp source-address-validation

Enable IP source guard.

Syntax	`[no] ip dhcp source-address-validation`
Defaults	Disabled.
Command Modes	INTERFACE
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

ip dhcp snooping vlan

Enable DHCP Snooping on one or more VLANs.

Syntax	`[no] ip dhcp snooping vlan` *`name`*
Parameters	*name* Enter the name of a VLAN on which to enable DHCP Snooping.
Defaults	Disabled.
Command Modes	CONFIGURATION
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	When enabled, the system begins creating entries in the binding table for the specified VLANs.

NOTE: Learning only happens if there is a trusted port in the VLAN.

Related Commands	ip dhcp snooping trust — configures an interface as trusted.

show ip dhcp snooping

Display the contents of the DHCP binding table.

Syntax	`show ip dhcp snooping binding`
Defaults	none
Command Modes	- EXEC - EXEC Privilege
Command History	Version 8.3.16.1 — Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	clear ip dhcp snooping — clears the contents of the DHCP binding table.

username

Establish an authentication system based on user names.

Syntax

```
username name [access-class access-list-name] [nopassword |
{password | secret} [encryption-type] password] [privilege
level] [role role-name]
```

If you do not want a specific user to enter a password, use the `nopassword` option.

To delete authentication for a user, use the `no username name` command.

Parameters

name	Enter a text string for the name of the user up to 63 characters.
access-class *access-list-name*	Enter the keywords `access-class` then the name of a configured access control list (either an IP access control list or MAC access control list).
nopassword	Enter the keyword `nopassword` to specify that the user should not enter a password.
password	Enter the keyword `password` then the `encryption-type` or the password.
secret	Enter the keyword `secret` then the `encryption-type` or the password.

encryption-type	Enter an encryption type for the `password` that you enter. • `0` directs the system to store the password as clear text. It is the default encryption type when using the `password` option. • `7` to indicate that a password encrypted using a DES hashing algorithm follows. This encryption type is available with the `password` option only. • `5` to indicate that a password encrypted using an MD5 hashing algorithm follows. This encryption type is available with the `secret` option only, and is the default encryption type for this option.
password	Enter a string up to 32 characters long.
privilege *level*	Enter the keyword `privilege` then a number from zero (0) to 15.
role *role-name*	Enter the keyword `role` followed by the role name to associate with that user ID.
secret	Enter the keyword `secret` then the encryption type.

Defaults

The default encryption type for the `password` option is **0**. The default encryption type for the `secret` option is **0**.

Command Modes

CONFIGURATION

Command History

Version 9.5(0.0)	Introduced the support for roles on the MXL 10/40GbE Switch.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To view the defined user names, use the `show running-config user` command.

Related Commands

password — specifies a password for users on terminal lines.

show running-config — views the current configuration.

userrole

Create user roles for the role-based security model.

Syntax

`userrole name inherit existing-role-name`

To delete a role name, use the no userrole *name* command. Note that the reserved role names may not be deleted.

Parameters

name	Enter a text string for the name of the user up to 63 characters. It cannot be one of the system defined roles (sysadmin, secadmin, netadmin, netoperator).
inherit *existing-role-name*	Enter the `inherit` keyword then specify the system defined role to inherit permissions from (sysadmin, secadmin, netadmin, netoperator).

Defaults

none

Command Modes

CONFIGURATION

Command History

Version 9.5(0.0)	Introduced on the Z9000, S6000, S4820T, S4810, MXL.

Usage Information

Instead of using the system defined user roles, you can create a new user role that best matches your organization. When you create a new user role, you first inherit permissions from one of the system defined roles. Otherwise you would have to create a user role from scratch. You then restrict commands or add commands to that role. For information about this topic, See *Modifying Command Permissions for Roles*.

NOTE: You can change user role permissions on system pre-defined user roles or user-defined user roles.

Important Points to Remember

Consider the following when creating a user role:

- Only the system administrator and user-defined roles inherited from the system administrator can create roles and usernames. Only the system administrator, security administrator, and roles inherited from these can use the `role` command to modify command permissions. The security administrator and roles inherited by security administrator can only modify permissions for commands they already have access to.
- Make sure you select the correct role you want to inherit.

NOTE: If you inherit a user role, you cannot modify or delete the inheritance. If you want to change or remove the inheritance, delete the user role and create it again. If the user role is in use, you cannot delete the user role.

Related Commands

role mode { { { **addrole | deleterole** } *role-name* } | **reset** } *command* – Modifies (adds or deletes) command permissions for newly created user roles and system defined roles.

48

sFlow

sFlow monitoring system includes an sFlow Agent and an sFlow Collector.

- The sFlow Agent combines the flow samples and interface counters into sFlow datagrams and forwards them to the sFlow Collector.
- The sFlow Collector analyses the sFlow Datagrams received from the different devices and produces a network-wide view of traffic flows.

Important Points to Remember

- Dell Networking OS recommends that the sFlow Collector be connected to the Dell Networking chassis through a line card port rather than the route processor module (RPM) Management Ethernet port.
- The system exports all sFlow packets to the sFlow Collector. A small sampling rate can equate to many exported packets. A backoff mechanism is automatically applied to reduce this amount. Some sampled packets may be dropped when the exported packet rate is high and the backoff mechanism is about to or is starting to take effect. The dropEvent counter, in the sFlow packet, is always zero.
- sFlow sampling is done on a per-port basis.
- Community list and local preference fields are not filled up in the extended gateway element in the sFlow datagram.
- The 802.1P source priority field is not filled up in the extended switch element in the sFlow datagram.
- Only Destination and Destination Peer AS numbers are packed in the dst-as-path field in the extended gateway element.
- If the packet being sampled is redirected using policy-based routing (PBR), the sFlow datagram may contain incorrect extended gateway/router information.
- The source virtual local area network (VLAN) field in the extended switch element is not packed if there is a routed packet.
- The destination VLAN field in the extended switch element is not packed if there is a multicast packet.
- The maximum number of packets that can be sampled and processed per second is:
    - 7500 packets when no extended information packing is enabled.
    - 7500 packets when only extended-switch information packing is enabled (refer to sflow extended-switch enable).
    - 1600 packets when you enable extended-router and/or extended-gateway information packing

sflow collector

Configure a collector device to which sFlow datagrams are forwarded.

Syntax

`sflow collector {ip-address} agent-addr {ip-address} [number [max-datagram-size number]] | [max-datagram-size number]`

To delete a configured collector, use the `no sflow collector {ip-address} agent-addr {ipv4-address} [number [max-datagram-size number]] | [max-datagram-size number]` command.

Parameters

sflow collector *ip-address*	Enter the IPv4 (A.B.C.D) of the sFlow collector device.
agent-addr *ip-address*	Enter the IPv4 (A.B.C.D) of the sFlow agent in the router.
number	(OPTIONAL) Enter the user datagram protocol (UDP) port number. The range is from 0 to 65535. The default is 6343.
max-datagram-size *number*	(OPTIONAL) Enter the keyword max-datagram-size then the size number in bytes. The range is from 400 to 1500. The default is **1400**.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

You can configure up to two sFlow collectors (IPv4 or IPv6). If two collectors are configured, traffic samples are sent to both.

The sFlow agent address is carried in a field in SFlow packets and is used by the collector to identify the sFlow agent.

In sFlow, the agent address is a single invariant IPv4 or IPv6 address used to identify the agent to the collector. It is usually assigned the address of a loopback interface on the agent, which provides invariance. The agent address is carried as a field in the payload of the sFlow packets.

As part of the sFlow-MIB, if the SNMP request originates from a configured collector, the system returns the corresponding configured agent IP in the MIB requests. The system checks to ensure that two entries are not configured for the same collector IP with a different agent IP. Should that happen, the system generates the following error: `%Error: Different agent-addr attempted for an existing collector.`

sflow enable (Global)

Enable sFlow globally.

Syntax	`sflow enable` To disable sFlow, use the `no sflow enable` command.
Defaults	Disabled.
Command Modes	CONFIGURATION
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	sFlow is disabled by default. In addition to this command, you must enable sFlow on individual interfaces where you want sFlow sampling.
Related Commands	sflow enable (Global) — enables sFlow on interfaces.

sflow enable (Interface)

Enable sFlow on interfaces.

Syntax	`sflow enable` To disable sFlow, use the `no sflow enable` command.
Defaults	Disabled.
Command Modes	INTERFACE
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	When you enable sFlow on an interface, flow sampling is done on any traffic going out of the interface. NOTE: After a physical port is a member of a LAG, it inherits the sFlow configuration from the LAG port.
Related Commands	sflow enable (Global) — turns sFlow on globally.

sflow extended-switch enable

Enable packing information on a switch only.

Syntax

```
sflow extended-switch enable
```

To disable packing information, use the `no sflow extended-switch [enable]` command.

Parameters

enable	Enter the keyword `enable` to enable global extended information.

Defaults Disabled.

Command Modes CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information The Dell Networking OS version 7.8.1.0 and later enhances the sflow implementation for real time traffic analysis to provide extended gateway information in cases where the destination IP addresses are learned by different routing protocols and for cases where the destination is reachable over ECMP.

Related Commands show sflow — displays the sFlow configuration.

sflow polling-interval (Global)

Set the sFlow polling interval at a global level.

Syntax

```
sflow polling-interval interval value
```

To return to the default, use the `no sflow polling-interval` *`interval`* command.

Parameters

interval value	Enter the interval value in seconds. The range is from 15 to 86400 seconds. The default is **20 seconds**.

Defaults **20 seconds**

Command Modes CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information The polling interval for an interface is the maximum number of seconds between successive samples of counters sent to the collector. This command changes the global default counter polling (20 seconds) interval. You can configure an interface to use a different polling interval.

sflow polling-interval (Global)

Set the sFlow polling interval at a global level.

Syntax

`sflow polling-interval interval value`

To return to the default, use the `no sflow polling-interval interval` command.

Parameters

interval value	Enter the interval value in seconds. The range is from 15 to 86400 seconds. The default is **20 seconds**.

Defaults

20 seconds

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The polling interval for an interface is the maximum number of seconds between successive samples of counters sent to the collector. This command changes the global default counter polling (20 seconds) interval. You can configure an interface to use a different polling interval.

sflow sample-rate (Global)

Change the global default sampling rate.

Syntax

`sflow sample-rate value`

To return to the default sampling rate, use the `no sflow sample-rate` command.

Parameters

value	Enter the sampling rate value. The range is from 256 to 8388608 packets. Enter values in powers of 2 only; for example, 4096, 8192, 16384, and so on. The default is **32768 packets**.

Defaults

32768 packets

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Sample-rate is the average number of packets skipped before the sample is taken. This command changes the global default sampling rate. You can configure an interface to use a different sampling rate than the global sampling rate. If the value entered is not a correct power of 2, the command generates an error message with the previous and next power of 2 value. Select one of these two packet numbers and re-enter the command.

Related Commands

sflow sample-rate (Interface) — changes the interface sampling rate.

sflow sample-rate (Interface)

Change the interface default sampling rate.

Syntax

`sflow sample-rate value`

To return to the default sampling rate, use the `no sflow sample-rate` command.

Parameters

value	Enter the sampling rate value. The range is from 256 to 8388608 packets. Enter values in powers of 2 only; for example, 4096, 8192, 16384, and so forth. The default is **the Global default sampling**.

Defaults

The Global default sampling.

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

This command changes the sampling rate for an interface. By default, the sampling rate of an interface is set to the same value as the current global default sampling rate. If the value you enter is not a correct power of 2, the command generates an error message with the previous and next power-of-2 value. Select one of these two number and re-enter the command.

Related Commands

sflow sample-rate (Global) — changes the sampling rate globally.

show sflow

Display the current sFlow configuration.

Syntax `show sflow [interface]`

Parameters

interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The dropEvent counter (sFlow samples dropped due to sub-sampling) shown in the following example always displays a value of zero.

Example

```
Dell#show sflow
sFlow services are enabled
Egress Mangement Interface sFlow services are disabled
Global default sampling rate: 2048
Global default counter polling interval: 20
Global extended information enabled: none
0 collectors configured
0 UDP packets exported
0 UDP packets dropped
0 sFlow samples collected

stack-unit 0 Port set 0
  Te 0/0: configured rate 256, actual rate 256
Dell#
Dell#show running-config sflow
!
sflow enable
sflow sample-rate 2048
Dell#show  running-config interface tengigabitethernet 0/0
!
interface TenGigabitEthernet 0/0
 no ip address
 sflow enable
 sflow sample-rate 256
 no shutdown
```

show sflow stack-unit

Display the sFlow information on a stack unit.

Syntax `show sflow stack-unit {unit number}`

Parameters

unit number	(OPTIONAL) Enter a unit number to view information on the stack unit in that slot. The range is from 0 to 5.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information The dropEvent counter (sFlow samples dropped due to sub-sampling) shown in the following example below always displays a value of zero.

Example

```
Dell#show sflow stack-unit 1
Stack-Unit 1
  Samples rcvd from h/w      :0
  Total UDP packets exported :0
UDP packets dropped          :0
Dell#
```

49

Service Provider Bridging

Service provider bridging is composed of virtual local area network (VLAN) Stacking, Layer 2 Protocol Tunneling, and Provider Backbone Bridging as described in the *Dell Networking OS Configuration Guide*.

This chapter includes commands for the Dell Networking operating software Layer 2 Protocol Tunneling (L2PT). L2PT enables protocols to tunnel through an 802.1q tunnel.

For more information, refer to VLAN Stacking, Spanning Tree Protocol (STP), and GARP VLAN Registration (GVRP).

Important Points to Remember

- L2PT is enabled at the interface VLAN-Stack VLAN level. For more information about Stackable VLAN (VLAN-Stacking) commands, refer to VLAN Stacking.
- The default behavior is to disable protocol packet tunneling through the 802.1q tunnel.
- Rate-limiting is required to protect against bridge protocol data units (BPDU) attacks.
- A port channel (including through link aggregation control protocol [LACP]) can be configured as a VLAN-Stack access or trunk port.
- Address resolution protocol (ARP) packets work as expected across the tunnel.
- Far-end failure detection (FEFD) works the same as with Layer 2 links.
- Protocols that use Multicast MAC addresses (for example, open shortest path first [OSPF]) work as expected and carry over to the other end of the VLAN-Stack VLAN.

debug protocol-tunnel

Enable debugging to ensure incoming packets are received and rewritten to a new MAC address.

Syntax

`debug protocol-tunnel interface {in | out | both} [vlan` *`vlan-id`*`] [count` *`value`*`]`

To disable debugging, use the `no debug protocol-tunnel interface {in | out | both} [vlan` *`vlan-id`*`] [count` *`value`*`]` command.

Parameters

interface	Enter one of the following interfaces and slot/port information: • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.

- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

in | out | both	Enter the keyword `in`, `out`, or `both` to debug incoming interfaces, outgoing interfaces, or both incoming and outgoing interfaces.
vlan *vlan-id*	Enter the keyword `vlan` then the VLAN ID. The range is from 1 to 4094.
count *value*	Enter the keyword `count` then the number of debug outputs. The range is from 1 to 100.

Defaults Debug disabled.

Command Modes EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

protocol-tunnel

Enable protocol tunneling on a stacked (Q-in-Q) VLAN for specified protocol packets.

Syntax `protocol-tunnel {rate-limit` *`rate`*`| stp}`

To disable protocol tunneling for a Layer 2 protocol, use the `no protocol-tunnel` command.

Parameters

rate-limit *rate*	Enter the keyword `rate-limit` then a number for the rate-limit for tunneled packets on the VMAN. The range is from 64 to 320.
stp	Enter the keyword `stp` to enable protocol tunneling on a spanning tree, including STP, MSTP, RSTP, and PVST.

Defaults none

Command Modes CONF-IF-VLAN

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#conf
Dell(conf)#interface vlan 2
Dell(conf-if-vl-2)#vlan-stack compatible
Dell(conf-if-vl-2)#member Gi1/2-3
Dell(conf-if-vl-2)#protocol-tunnel stp
Dell(conf-if-vl-2)#protocol-tunnel enable
```

Related Command	show protocol-tunnel — displays tunneling information for all VLANs.

protocol-tunnel destination-mac

Overwrite the BPDU destination MAC address with a specific value.

Syntax	`protocol-tunnel destination-mac xstp address`
Parameters	**stp** Change the default destination MAC address used for L2PT to another value.
Defaults	The default destination MAC is 01:01:e8:00:00:00.
Command Modes	CONFIGURATION
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	When you enable VLAN-Stacking, no protocol packets are tunneled.
Related Command	show protocol-tunnel — displays tunneling information for all VLANs.

protocol-tunnel enable

Enable protocol tunneling globally on the system.

Syntax	`protocol-tunnel enable` To disable protocol tunneling, use the `no protocol-tunnel enable` command.
Defaults	Disabled.
Command Modes	CONFIGURATION
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	The system must have the default CAM profile with the default microcode before you enable L2PT.

protocol-tunnel rate-limit

Enable traffic rate limiting per box.

Syntax	`protocol-tunnel rate-limit` *`rate`* To reset the rate limit to the default, use the `no protocol-tunnel rate-limit` *`rate`* command.
Parameters	*rate*: Enter the rate in frames per second. The range is from 75 to 3000. The default is **75**.
Defaults	**75** frames per second.
Command Modes	CONFIGURATION
Command History	Version 9.2(0.0): Introduced on the MXL 10/40GbE Switch IO Module.
Example	see below
Related Commands	show protocol-tunnel — displays tunneling information for all VLANs. show running-config — displays the current configuration.

Example:

```
Dell#
Dell#conf
Dell(conf)#protocol-tunnel rate-limit 1000
Dell(conf)#
```

show protocol-tunnel

Display protocol tunnel information for all or a specified VLAN-Stack VLAN.

Syntax	`show protocol-tunnel [vlan` *`vlan-id`*`]`
Parameters	vlan *vlan-id*: (OPTIONAL) Enter the keyword `vlan` then the VLAN ID to display information for the one VLAN. The range is from 1 to 4094.
Defaults	none
Command Modes	EXEC
Command History	Version 9.2(0.0): Introduced on the MXL 10/40GbE Switch IO Module.
Example	see below

Example:

```
Dell#show protocol-tunnel
System Rate-Limit: 75 frames/second
VLAN  Protocols   Interface
1000  STP,PVST    Gi 5/7,Gi 5/6
```

```
1001  LLDP,GVRP   Gi 5/7,Gi 5/6
1002  MMRP,MVRP   Gi 5/7,Gi 5/6
1003  LACP,DOT1X  Gi 5/7,Gi 5/6
1004  OAM,PAUSE   Gi 5/7,Gi 5/6
1005  E-LMI       Gi 5/7,Gi 5/6
```

Example (Specific VLAN)

```
Dell#show protocol-tunnel vlan 2
System Rate-Limit: 1000 Frames/second
Interface  Vlan  Protocol(s)
Gi1/2      2     STP, PVST
Dell#
```

Related Commands

show running-config — displays the current configuration.

50

Simple Network Management Protocol (SNMP) and Syslog

This chapter contains commands to configure and monitor the simple network management protocol (SNMP) v1/v2/v3 and Syslog.

The chapter contains the following sections:

- SNMP Commands
- Syslog Commands

SNMP Commands

The following SNMP commands are available in the Dell Networking OS.

The simple network management protocol (SNMP) is used to communicate management information between the network management stations and the agents in the network elements. The system supports SNMP versions 1, 2c, and 3, supporting both read-only and read-write modes. The system sends SNMP traps, which are messages informing an SNMP management system about the network. The system supports up to 16 SNMP trap receivers.

Important Points to Remember

- Typically, 5-second timeout and 3-second retry values on an SNMP server are sufficient for both local area network (LAN) and wide area network (WAN) applications. If you experience a timeout with these values, the recommended best practice on Dell Networking switches (to accommodate their high port density) is to increase the timeout and retry values on your SNMP server to the following:
  - SNMP Timeout — greater than 3 seconds.
  - SNMP Retry count — greater than 2 seconds.
- If you are using access control lists (ACLs) in an SNMP v3 configuration, group ACL overrides user ACL if the user is part of that group.
- SNMP operations are not supported on a virtual local area network (VLAN).

clear logging auditlog

Clears audit log.

Syntax

```
clear logging auditlog
```

Defaults	none
Command Modes	EXEC
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*. The following is a list of the Dell Networking OS version history for this command.

Version 9.5(0.0)	Introduced on the S4810, S4820T, S6000, Z9000, and MXL.

Example

```
Dell(conf)#clear logging auditlog
```

Related Commands

show logging auditlog — displays audit log

show snmp

Display the status of SNMP network elements.

Syntax

```
show snmp
```

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show snmp
  32685 SNMP packets input
      0 Bad SNMP version errors
      0 Unknown community name
      0 Illegal operation for community name supplied
      0 Encoding errors
  96988 Number of requested variables
      0 Number of altered variables
  31681 Get-request PDUs
    968 Get-next PDUs
      0 Set-request PDUs
  61727 SNMP packets output
      0 Too big errors (Maximum packet size 1500)
      9 No such name errors
      0 Bad values errors
      0 General errors
  32649 Response PDUs
  29078 Trap PDUs
Dell#
```

Related Commands

snmp-server community — enables the SNMP and set community string.

show snmp engineID

Display the identification of the local SNMP engine and all remote engines that are configured on the router.

Syntax

```
show snmp engineID
```

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show snmp engineID
Local SNMP engineID: 0000178B02000001E80214A8
Remote Engine ID        IP-addr       Port
80001F88043132333435    172.31.1.3    5009
80001F88043938373635    172.31.1.3    5008

Dell#
```

Related Commands

snmp-server engineID — configures local and remote SNMP engines on the router.

show snmp group

Display the group name, security model, status, and storage type of each group.

Syntax

```
show snmp group
```

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following Example displays a group named *ngroup*. The *ngroup* has a security model of version 3 (v3) with authentication (`auth`), the read and notify name is *nview* with no write view name specified, and finally the row status is active.

Example

```
Dell#show snmp group

groupname: ngroup          security model: v3 auth
readview : nview           writeview: no write view specified
notifyview: nview
row status: active

Dell#
```

Related Commands	snmp-server group — configures an SNMP server group.

show snmp user

Display the information configured on each SNMP user name.

Syntax `show snmp user`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show snmp user
  User name: v1v2creadu
  Engine ID: 0000178B02000001E80214A8
  storage-type: nonvolatile     active
  Authentication Protocol: None
  Privacy Protocol: None

Dell#
```

snmp ifmib ifalias long

Display the entire description string through the Interface MIB, which would be truncated otherwise to 63 characters.

Syntax `snmp ifmib ifalias long`

Defaults Interface description truncated beyond 63 characters.

Command Modes CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
!----command run on host connected to switch:------!
> snmpwalk -c public 10.10.10.130 .1.3.6.1.2.1.31 | grep -i
alias | more
IF-MIB::ifAlias.134530304 = STRING: This is a port connected
to Router2. This is a
port connected to
IF-MIB::ifAlias.134792448 = STRING:

!----command run on Force10 switch:-----------!
Dell#snmp ifmib ifalias long

!----command run on server connected to switch:------!
```

```
> snmpwalk -c public 10.10.10.130 .1.3.6.1.2.1.31 | grep -i
alias | more
IF-MIB::ifAlias.134530304 = STRING: This is a port connected
to Router2. This is a
port connected to Router2. This is a port connected to
Router2. This is a port
connected to Router2. This is a port connected to Router2.
IF-MIB::ifAlias.134792448 = STRING:
```

snmp-server community

Configure a new community string access for SNMPv1 v2 and v3.

Syntax

`snmp-server community` *`community-name`* `{ro | rw} [security-name` *`name`*`][`*`access-list-name`*`]`

To remove access to a community, use the `no snmp-server community` *`community-string`* `{ro | rw} [security-name` *`name`* `[`*`access-list-name`*`]` command.

Parameters

community-name	Enter a text string (up to 20 characters long) to act as a password for SNMP.
ro	Enter the keyword `ro` to specify read-only permission.
rw	Enter the keyword `rw` to specify read-write permission.
security-name *name*	(Optional) Enter the keywords `security-name` then the security name as defined by the community MIB.
access-list-name	(Optional) Enter a standard IPv4 access list name (a string up to 16 characters long).

Defaults

none

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following example configures a community named *public* that is mapped to the security named *guestuser* with Read Only (`ro`) permissions.

The `security-name` parameter maps the community string to an SNMPv3 user/ security name as defined by the community MIB.

If a community string is configured without a `security-name` (for example, `snmp-server community public ro`), the community is mapped to a default security-name/group:

- `v1v2creadu / v1v2creadg` — maps to a community with `ro` (read-only) permissions.

- `v1v2cwriteu/ v1v2cwriteg` — maps to a community with `rw` (read-write) permissions.

The `community-name` parameter indexes this command.

If you do not configure the `snmp-server community` command, you cannot query SNMP data. Only Standard IPv4 ACL and IPv6 ACL is supported in the optional `access-list-name`.

The command options `ipv6`, `security-name`, and `access-list-name` are recursive. In other words, each option can, in turn, accept any of the three options as a sub-option, and each of those sub-options can accept any of the three sub-options as a sub-option, and so forth. The second Example shows the creation of a standard IPv4 ACL called *snmp-ro-acl* and then assigning it to the SNMP community *guest*.

NOTE: For IPv6 ACLs, only IPv6 and UDP types are valid for SNMP; TCP and ICMP rules are not valid for SNMP. In IPv6 ACLs, port rules are not valid for SNMP.

Example

```
Dell#config
Dell(conf)# snmp-server community public ro
Dell(conf)# snmp-server community guest ro security-name
guestuser
Dell(conf)#
```

Example

```
Dell(conf)# ip access-list standard snmp-ro-acl
Dell(config-std-nacl)#seq 5 permit host 10.10.10.224
Dell(config-std-nacl)#seq 10 deny any count
!

Dell(conf)#snmp-server community guest ro snmp-ro-acl
Dell(conf)#
```

Related Commands

ip access-list standard — names (or selects) a standard access list to filter based on IP address.

show running-config — displays the current SNMP configuration and defaults.

snmp-server contact

Configure contact information for troubleshooting this SNMP node.

Syntax

`snmp-server contact text`

To delete the SNMP server contact information, use the `no snmp-server contact` command.

Parameters

text	Enter an alphanumeric text string, up to 55 characters long.

Defaults	none	
Command Modes	CONFIGURATION	
Command History	**Version 8.3.16.1**	Introduced on the MXL 10/40GbE Switch IO Module.

snmp-server enable traps

Enable SNMP traps.

Syntax

`snmp-server enable traps [`*`notification-type`*`] [`*`notification-option`*`]`

To disable traps, use the `no snmp-server enable traps [`*`notification-type`*`] [`*`notification-option`*`]` command.

Parameters

notification-type

Enter the type of notification from the following list:

- `ecfm` — Notification of changes to ECFM.
- `entity` — Notification of changes to entity.
- `envmon` — For Dell Networking device notifications when an environmental threshold is exceeded.
- `eoam` — Notification of changes to the EOAM state.
- `ets` — Notification of changes to the ets traps.
- `fips` — Notification of changes to the FIP snooping state.
- `lacp` — Notification of changes.
- `pfc` — Notification of changes to pfc traps.
- `snmp` — Notification of RFC 1157 traps.
- `stp` — Notification of a state change in the spanning tree protocol (RFC 1493).
- `vrrp` — Notification of a state change in a VRRP group.
- `xstp` — Notification of a state change in MSTP (802.1s), RSTP (802.1w), and PVST+.

notification-option

For the `envmon` notification-type, enter one of the following optional parameters:

- `temperature`

For the `snmp` notification-type, enter one of the following optional parameters:

- `authentication`
- `coldstart`

- `linkdown`
- `linkup`

Defaults	Not enabled.
Command Modes	CONFIGURATION
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	The system supports up to 16 SNMP trap receivers. If you do not configure this command, no traps controlled by this command are sent. If you do not specify a `notification-type` and `notification-option`, all traps are enabled.
Related Commands	snmp-server community — enables SNMP and sets the community string.

snmp-server engineID

Configure the name for both the local and remote SNMP engines on the router.

Syntax

`snmp-server engineID [local` *`engineID`*`] [remote` *`ip-address`* `udp-port` *`port-number engineID`*`]`

To return to the default, use the `no snmp-server engineID [local` *`engineID`*`] [remote` *`ip-address`* `udp-port` *`port-number engineID`*`]` command.

Parameters

local *engineID*	Enter the keyword `local` then the engine ID number that identifies the copy of the SNMP on the local device. Format (as specified in RFC 3411): 12 octets. • The first four octets are set to the private enterprise number. • The remaining eight octets are the MAC address of the chassis.
remote *ip-address*	Enter the keyword `remote` then the IP address that identifies the copy of the SNMP on the remote device.
udp-port *port-number engineID*	Enter the keywords `udp-port` then the user datagram protocol (UDP) port number on the remote device. The range is from 0 to 65535. The default is **162**.

Defaults

As above.

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Changing the value of the SNMP Engine ID has important side effects. A user's password (entered on the command line) is converted to a message digest algorithm (MD5) or secure hash algorithm (SHA) security digest. This digest is based on both the password and the local Engine ID. The command line password is then destroyed, as required by RFC 2274. Because of this deletion, if the local value of the Engine ID changes, the security digests of SNMPv3 users is invalid and you must reconfigure the users.

For the remote Engine ID, the host IP and UDP port are the indexes to the command that are matched to either overwrite or remove the configuration.

Related Commands

show snmp engineID — displays the SNMP engine and all the remote engines that are configured on the router.

show running-config — displays the SNMP running configuration.

snmp-server group

Configure a new SNMP group or a table that maps SNMP users to SNMP views.

Syntax

```
snmp-server group [group_name {1 | 2c | 3 {auth | noauth |
priv}}] [read name] [write name] [notify name] [ access-list-
name | access-list-name]]
```

To remove a specified group, use the `no snmp-server group [group_name {v1 | v2c | v3 {auth | noauth | priv}}] [read name] [write name] [notify name] [access-list-name | access-list-name]]` command.

Parameters

group_name	Enter a text string (up to 20 characters long) as the name of the group. The following groups are created for mapping to read/write community/security-names (defaults): • `v1v2creadg` — maps to a community/security-name with `ro` permissions. • `1v2cwriteg` — maps to a community/security-name `rw` permissions.
1 | 2c | 3	(OPTIONAL) Enter the security model version number (`1`, `2c`, or `3`):

- `1` is the least secure version.
- `3` is the most secure of the security modes.
- `2c` allows transmission of informs and counter 64, which allows for integers twice the width of what is normally allowed.

The default is **1**.

auth	(OPTIONAL) Enter the keyword `auth` to specify authentication of a packet without encryption.
noauth	(OPTIONAL) Enter the keyword `noauth` to specify no authentication of a packet.
priv	(OPTIONAL) Enter the keyword `priv` to specify both authentication and then scrambling of the packet.
read *name*	(OPTIONAL) Enter the keyword `read` then a name (a string of up to 20 characters long) as the read view name. The default is **GlobalView** and is assumed to be every object belonging to the internet (1.3.6.1) OID space.
write *name*	(OPTIONAL) Enter the keyword `write` then a name (a string of up to 20 characters long) as the write view name.
notify *name*	(OPTIONAL) Enter the keyword `notify` then a name (a string of up to 20 characters long) as the notify view name.
access-list-name	(Optional) Enter the standard IPv4 access list name (a string up to 16 characters long).

Defaults

As above.

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following Example specifies the group named *harig* as a version 3 user requiring both authentication and encryption and read access limited to the read named *rview*.

NOTE: The number of configurable groups is limited to 16 groups.

Example

```
Dell#conf
Dell(conf)# snmp-server group harig 3 priv read rview
Dell#
```

Related Commands

show snmp group — displays the group name, security model, view status, and storage type of each group.

show running-config — displays the SNMP running configuration.

snmp-server host

Configure the recipient of an SNMP trap operation.

Syntax

`snmp-server host ip-address [traps | informs] [version 1 | 2c | 3] [auth | no auth | priv] [community-string] [udp-port port-number] [notification-type]`

To remove the SNMP host, use the `no snmp-server host ip-address [traps | informs] [version 1 | 2c | 3] [auth | noauth | priv] [community-string] [udp-port number] [notification-type]` command.

Parameters

ip-address	Enter the keyword `host` then the IP address of the host (configurable hosts is limited to 16).
traps	(OPTIONAL) Enter the keyword `traps` to send trap notifications to the specified host. The default is **traps**.
informs	(OPTIONAL) Enter the keyword `informs` to send inform notifications to the specified host. The default is **traps**.
version 1 | 2c | 3	(OPTIONAL) Enter the keyword version to specify the security model then the security model version number `1`, `2c`, or `3`: • Version `1` is the least secure version. • Version `3` is the most secure of the security modes. • Version `2c` allows transmission of informs and counter 64, which allows for integers twice the width of what is normally allowed. The default is version **1**.
auth	(OPTIONAL) Enter the keyword `auth` to specify authentication of a packet without encryption.
noauth	(OPTIONAL) Enter the keyword `noauth` to specify no authentication of a packet.
priv	(OPTIONAL) Enter the keyword `priv` to specify both authentication and then scrambling of the packet.
community-string	Enter a text string (up to 20 characters long) as the name of the SNMP community. NOTE: For version 1 and version 2c security models, this string represents the name of the SNMP community. The string can be set using this command; however, Dell Networking OS recommends setting the community string using the `snmp-server community` command before executing this command. For version 3 security model, this string is the USM user security name.

udp-port *port-number*	(OPTIONAL) Enter the keywords `udp-port` then the port number of the remote host to use. The range is from 0 to 65535. The default is **162**.
notification-type	(OPTIONAL) Enter one of the following keywords for the type of trap to send to the host: • `ecfm` — Notification of ECFM state changes. • `entity` — Notification of entity changes. • `envmon` — Environment monitor trap. • `eoam` — Notificaiton of EOAM state changes. • `ets` — Notification of ets trap changes. • `fips` — Notification of FIP snooping state changes. • `lacp` — Notificaiton of LACP state changes. • `snmp` — SNMP notification (RFC 1157). • `stp` — Spanning tree protocol notification (RFC 1493). • `vrrp` — State change in a VRRP group. • `xstp` — State change in MSTP (802.1s), RSTP (802.1w), and PVST+. The default is all trap types are sent to host.

Defaults As above.

Command Modes CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

In order to configure the router to send SNMP notifications, enter at least `one snmp-server host` command. If you enter the command with no keywords, all trap types are enabled for the host. If you do not enter an `snmp-server host` command, no notifications are sent.

In order to enable multiple hosts, issue a separate `snmp-server host` command for each host. You can specify multiple notification types in the command for each host.

When multiple `snmp-server host` commands are given for the same host and type of notification (trap or inform), each succeeding command overwrites the previous command. Only the last `snmp-server host` command is in effect. For example, if you enter an `snmp-server host inform` command for a host and then enter another `snmp-server host inform` command for the same host, the second command replaces the first command.

The `snmp-server host` command is used with the `snmp-server enable` command. Use the `snmp-server enable` command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one `snmp-server enable` command and the `snmp-server host` command for that host must be enabled.

NOTE: For v1 / v2c trap configuration, if the community-string is not defined using the `snmp-server community` command prior to using this command, the default form of the `snmp-server community` command automatically is configured with the community-name the same as specified in the `snmp-server host` command.

Configuring Informs

To send an inform, use the following steps:

1. Configure a remote engine ID.
2. Configure a remote user.
3. Configure a group for this user with access rights.
4. Enable traps.
5. Configure a host to receive informs.

Related Commands

snmp-server enable traps — enables SNMP traps.

snmp-server community — configures a new community SNMPv1 or SNMPv2c.

snmp-server location

Configure the location of the SNMP server.

Syntax

`snmp-server location text`

To delete the SNMP location, use the `no snmp-server location` command.

Parameters

text	Enter an alpha-numeric text string, up to 55 characters long.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

snmp-server packetsize

Set the largest SNMP packet size permitted. Wen the SNMP server is receiving a request or generating a reply, use the `snmp-server packetsize global configuration` command.

Syntax	`snmp-server packetsize` *`byte-count`*
Parameters	*byte-count* — Enter one of the following values 8, 16, 24 or 32. Packet sizes are 8000 bytes, 16000 bytes, 32000 bytes, and 64000 bytes.
Defaults	**8**
Command Modes	CONFIGURATION
Command History	Version 8.3.16.1 — Introduced on the MXL 10/40GbE Switch IO Module.

snmp-server trap-source

Configure a specific interface as the source for SNMP traffic.

Syntax

`snmp-server trap-source` *`interface`*

To disable sending traps out a specific interface, use the `no snmp trap-source` command.

Parameters

interface	Enter the following keywords and slot/port or number information: • For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

Defaults	The IP address assigned to the management interface is the default.
Command Modes	CONFIGURATION
Command History	Version 8.3.16.1 — Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	To enable this `snmp-server trap-source` command, configure an IP address on the interface and enable the interface configured as an SNMP trap source.

Related Commands

snmp-server community — sets the community string.

snmp-server user

Configure a new user to an SNMP group.

Syntax

```
snmp-server user name {group_name remote ip-address udp-port
port-number} [1 | 2c | 3] [encrypted] [auth {md5 | sha} auth-
password] [priv des56 | aes128-cfb} priv-password [access
access-list-name | ipv6 access-list-name | access-list-name
ipv6 access-list-name]
```

To remove a user from the SNMP group, use the `no snmp-server user name {group_name remote ip-address udp-port port-number} [1 | 2c | 3] [encrypted] [auth {md5 | sha} auth-password] [priv des56 | aes128-cfb} priv password] [access access-list-name | ipv6 access-list-name]` command.

Parameters

name	Enter the name of the user (not to exceed 20 characters), on the host that connects to the agent.
group_name	Enter a text string (up to 20 characters long) as the name of the group. The following groups are created for mapping to read/write community/security-names (defaults): • `v1v2creadu` — maps to a community with `ro` permissions. • `1v2cwriteu` — maps to a community `rw` permissions.
remote *ip-address*	Enter the keywords `udp-port` then the user datagram protocol (UDP) port number on the remote device. The range is from 0 to 65535. The default is **162**.
udp-port *port-number*	Enter the keywords `udp-port` then the UDP (User Datagram Protocol) port number on the remote device. The range is from 0 to 65535. The default is **162**.
1 | 2c | 3	(OPTIONAL) Enter the security model version number (`1`, `2c`, or `3`): • `1` is the least secure version. • `3` is the most secure of the security modes. • `2c` allows transmission of informs and counter 64, which allows for integers twice the width of what is normally allowed. The default is **1**.

encrypted	(OPTIONAL) Enter the keyword `encrypted` to specify the password appear in encrypted format (a series of digits, masking the true characters of the string).
auth	(OPTIONAL) Enter the keyword `auth` to specify authentication of a packet without encryption.
md5 | sha	(OPTIONAL) Enter the keyword `md5` or `sha` to designate the authentication level. • `md5` — Message Digest Algorithm • `sha` — Secure Hash Algorithm
auth-password	(OPTIONAL) Enter a text string (up to 20 characters long) password that enables the agent to receive packets from the host and to send packets to the host. Minimum: eight characters long.
priv des56	(OPTIONAL) Enter the keywords `priv des56` to initiate a privacy authentication level setting using the CBC-DES privacy authentication algorithm (des56).
aes128	(OPTIONAL) Enter the keyword `aes128` to initiate the AES128-CFB encryption algorithm for transmission of SNMP packets.
priv password	(OPTIONAL) Enter a text string (up to 20 characters long) password that enables the host to encrypt the contents of the message it sends to the agent and decrypt the contents of the message it receives from the agent. Minimum: eight characters long.
access-list-name	(Optional) Enter the standard IPv4 access list name (a string up to 16 characters long).

Defaults

If no authentication or privacy option is configured, then the messages are exchanged (attempted anyway) without any authentication or encryption.

Command Modes

CONFIGURATION

Command History

Version 9.3(0.0)	Added support for the AES128-CFB encryption algorithm on the MXL 10/40GbE Switch IO Module platform.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

No default values exist for authentication or privacy algorithms and no default password exists. If you forget a password, you cannot recover it; the user must be reconfigured. You can specify either a plain-text password or an encrypted cypher-text password. In either case, the password is stored in the configuration in an encrypted form and displayed as encrypted in the `show running-config` command.

If you have an encrypted password, you can specify the encrypted string instead of the plain-text password. The following command is an Example of how to specify the command with an encrypted string.

NOTE: The number of configurable users is limited to 16.

Example

```
Dell# snmp-server user privuser v3group v3 encrypted auth md5
9fc53d9d908118b2804fe80e3ba8763d priv des56
d0452401a8c3ce42804fe80e3ba8763d
```

Usage Information

The following command is an example of how to enter a plain-text password as the string `authpasswd` for user `authuser` of group `v3group`.

Example

```
Dell#conf
Dell(conf)# snmp-server user authuser v3group v3 auth md5
authpasswd
```

Usage Information

The following command configures a remote user named *n3user* with a v3 security model and a security level of `authNOPriv`.

Example

```
Dell#conf
Dell(conf)# snmp-server user n3user ngroup remote 172.31.1.3
udp-port 5009 3
auth md5 authpasswd
```

Related Commands

show snmp user — displays the information configured on each SNMP user name.

snmp-server user (for AES128-CFB Encryption)

Specify that AES128-CFB encryption algorithm needs to be used for transmission of SNMP information. The Advanced Encryption Standard (AES) Cipher Feedback (CFB) 128-bit encryption algorithm is in compliance with RFC 3826. RFCs for SNMPv3 define two authentication hash algorithms, namely, HMAC-MD5-96 and HMAC-SHA1-96. These are the full forms or editions of the truncated versions, namely, HMAC-MD5 and HMAC-SHA1 authentication algorithms.

Syntax

`snmp-server user` *`name`* `{`*`group_name`* `remote` *`ip-address`* `udp-port` *`port-number`*`} [1 | 2c | 3] [encrypted] [auth {md5 | sha}` *`auth-password`*`] [priv {des56 | aes128-cfb}` *`priv- password`*`] [access` *`access-list-name`* `| ipv6` *`access-list-name`* `|` *`access-list-name`* `ipv6` *`access-list-name`*`]`

To remove a user from the SNMP group, use the `no snmp-server user` *`name`* `{`*`group_name`* `remote` *`ip-address`* `udp-port` *`port-number`*`} [1 | 2c | 3] [encrypted] [auth {md5 | sha}` *`auth-password`*`] [priv {des56 | aes128-cfb}` *`priv-password`*`] [access` *`access-list-name`* `| ipv6` *`access-list-name`* `|` *`access-list-name`* `ipv6` *`access-list-name`*`]` command.

Parameters

auth-password	(OPTIONAL) Enter a text string (up to 20 characters long) password that enables the agent to receive packets from the

	host and to send packets to the host. Minimum: eight characters long.
aes128	(OPTIONAL) Enter the keyword `aes128` to initiate the AES128-CFB encryption algorithm for transmission of SNMP packets.
priv-password	(OPTIONAL) Enter a text string (up to 20 characters long) password that enables the host to encrypt the contents of the message it sends to the agent and to decrypt the contents of the message it receives from the agent. Minimum: eight characters long.

Defaults

If no authentication or privacy option is configured, then the messages are exchanged (attempted anyway) without any authentication or encryption.

Command Modes

CONFIGURATION

Command History

Version 9.3(0.0)	Added support for the AES128-CFB encryption algorithm on MXL

Usage Information

To enable robust, effective protection and security for SNMP packets transferred between the server and the client, you can use the `snmp-server user username group groupname 3 auth authentication-type auth-password priv aes128 priv-password` to specify that AES128-CFB encryption algorithm needs to be used.

You cannot modify the FIPS mode if SNMPv3 users are already configured and present in the system. An error message is displayed if you attempt to change the FIPS mode by using the `fips mode enable` command in Global Configuration mode. You can enable or disable FIPS mode only if SNMPv3 users are not previously set up. Otherwise, you must remove the previously configured users before you change the FIPS mode.

Example

```
Dell# snmp-server user privuser v3group v3 encrypted auth md5
9fc53d9d908118b2804fe80e3ba8763d priv aes128
d0452401a8c3ce42804fe80e3ba8763d
```

Related Commands

show snmp user — Displays the information configured on each SNMP user name.

snmp-server view

Configure an SNMPv3 view.

Syntax

`snmp-server view view-name oid-tree {included | excluded}`

To remove an SNMPv3 view, use the `no snmp-server view view-name oid-tree {included | excluded}` command.

Parameters	*view-name*	Enter the name of the view (not to exceed 20 characters).
	oid-tree	Enter the OID sub tree for the view (not to exceed 20 characters).
	included	(OPTIONAL) Enter the keyword `included` to include the MIB family in the view.
	excluded	(OPTIONAL) Enter the keyword `excluded` to exclude the MIB family in the view.

Defaults	none
Command Modes	CONFIGURATION
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	The `oid-tree` variable is a full sub-tree starting from 1.3.6 and cannot specify the name of a sub-tree or a MIB. The following Example configures a view named *rview* that allows access to all objects under 1.3.6.1.
Example	`Dell#(conf) snmp-server view rview 1.3.6.1 included`
Related Commands	show running-config — displays the SNMP running configuration.

snmp trap link-status

Enable the interface to send SNMP link traps, which indicate whether the interface is up or down.

Syntax	`snmp trap link-status` To disable sending link trap messages, use the `no snmp trap link-status` command.
Defaults	Enabled.
Command Modes	INTERFACE
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	If the interface is expected to flap during normal usage, you could disable this command.

Syslog Commands

The following commands allow you to configure logging functions on all Dell Networking switches.

clear logging

Clear the messages in the logging buffer.

Syntax	`clear logging`
Defaults	none
Command Modes	EXEC Privilege
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	show logging — displays logging settings and system messages in the internal buffer.

default logging buffered

Return to the default setting for messages logged to the internal buffer.

Syntax	`default logging buffered`
Defaults	**size = 40960; level = 7 or debugging**
Command Modes	CONFIGURATION
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	default logging buffered — sets the logging buffered parameters.

default logging console

Return the default settings for messages logged to the console.

Syntax	`default logging console`
Defaults	**level = 7 or debugging**
Command Modes	CONFIGURATION

Command History		
	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

logging console — sets the logging console parameters.

logging extended

Logs security and audit events to a system log server.

Syntax

```
logging extended
```

Defaults

none

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version 9.5(0.0)	Introduced on the S4810, S4820T, S6000, Z9000, and MXL.

Usage Information

This command is available with or without RBAC enabled. When RBAC is enabled you can restrict access to audit and security logs based on the CLI sessions' user roles. If extended logging is disabled, you can only view system events, regardless of RBAC user role.

When you enabled RBAC and extended logging:

- Only the system administrator role can execute this command.
- The system administrator and system security administrator roles can view security events and system events.
- The system administrator role can view audit, security, and system events.
- The network administrator and network operator roles can view system events.

Examples

```
Dell(conf)#logging extended
```

Related Commands

show logging auditlog — displays audit log, clear logging auditlog— clears audit log

default logging monitor

Return to the default settings for messages logged to the terminal.

Syntax	`default logging monitor`
Defaults	**level = 7 or debugging**
Command Modes	CONFIGURATION
Command History	Version 8.3.16.1 — Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	logging monitor — sets the logging monitor parameters. terminal monitor — sends system messages to the terminal/monitor.

default logging trap

Return to the default settings for logging messages to the Syslog servers.

Syntax	`default logging trap`
Defaults	**level = 6 or informational**
Command Modes	CONFIGURATION
Command History	Version 8.3.16.1 — Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	logging trap — limit messages logged to the Syslog servers based on severity.

logging

Configure an IP address or host name of a Syslog server where logging messages are sent. You can configure multiple logging servers of both IPv4 and/or IPv6.

Syntax

```
logging {ip-address | ipv6-address |hostname} {{udp {port}} |
{tcp {port}}
```

To disable logging, use the `no logging` command.

Parameters

ip-address	Enter the IPv4 address in dotted decimal format.
ipv6-address	Enter the IPv6 address in the x:x:x:x::X format.

NOTE: The :: notation specifies successive hexadecimal fields of zeros.

hostname	Enter the name of a host already configured and recognized by the switch.
udp	Enter the keyword `udp` to enable transmission of log message over UDP followed by port number. The default port is 514
tcp	Enter the keyword `tcp` to enable transmission of log message over TCP followed by port number.

Defaults Disabled.

Command Modes CONFIGURATION

Command History

Version 9.5(0.0)	Introduced **udp** and **tcp** keywords on the MXL 10/40GbE Switch.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

logging on — enables the logging asynchronously to logging buffer, console, Syslog server, and terminal lines.

logging trap — enables logging to the Syslog server based on severity.

logging buffered

Enable logging and specify which messages are logged to an internal buffer. By default, all messages are logged to the internal buffer.

Syntax `logging buffered [level] [size]`

To return to the default values, use the `default logging buffered` command.

To disable logging stored to an internal buffer, use the `no logging buffered` command.

Parameters

level	(OPTIONAL) Indicate a value from 0 to 7 or enter one of the following equivalent words: `emergencies`, `alerts`, `critical`, `errors`, `warnings`, `notifications`, `informational`, or `debugging`. The default is **7** or **debugging**.
size	(OPTIONAL) Indicate the size, in bytes, of the logging buffer. The number of messages buffered depends on the size of each message. The range is from 40960 to 524288. The default is **40960 bytes**.

Defaults	level = **7**; size = **40960 bytes**
Command Modes	CONFIGURATION
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	When you decrease the buffer size, all messages stored in the buffer are lost. Increasing the buffer size does not affect messages stored in the buffer.
Related Commands	clear logging — clears the logging buffer. default logging buffered — returns the logging buffered parameters to the default setting. show logging — displays the logging setting and system messages in the internal buffer.

logging console

Specify which messages are logged to the console.

Syntax	`logging console [level]` To return to the default values, use the `default logging console` command. To disable logging to the console, use the `no logging console` command.	
Parameters	*level*	(OPTIONAL) Indicate a value from 0 to 7 or enter one of the following parameters: `emergencies`, `alerts`, `critical`, `errors`, `warnings`, `notifications`, `informational`, or `debugging`. The default is **7** or **debugging**.
Defaults	level = **7**; size = **debugging**	
Command Modes	CONFIGURATION	
Command History	**Version 8.3.16.1**	Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	clear logging — clears the logging buffer. default logging console — returns the logging console parameters to the default setting. show logging — displays the logging setting and system messages in the internal buffer.	

logging facility

Configure the Syslog facility used for error messages sent to Syslog servers.

Syntax

`logging facility [facility-type]`

To return to the default values, use the `no logging facility` command.

Parameters

facility-type

(OPTIONAL) Enter one of the following parameters:

- `auth` (authorization system)
- `cron` (Cron/at facility)
- `deamon` (system deamons)
- `kern` (kernel)
- `local0` (local use)
- `local1` (local use)
- `local2` (local use)
- `local3` (local use)
- `local4` (local use)
- `local5` (local use)
- `local6` (local use)
- `local7` (local use)
- `lpr` (line printer system)
- `mail` (mail system)
- `news` (USENET news)
- `sys9` (system use)
- `sys10` (system use)
- `sys11` (system use)
- `sys12` (system use)
- `sys13` (system use)
- `sys14` (system use)
- `syslog` (Syslog process)
- `user` (user process)
- `uucp` (Unix to Unix copy process)

The default is **local7**.

Defaults

local7

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands	logging — enables logging to a Syslog server. logging on — enables logging.

logging history

Specify which messages are logged to the history table of the switch and the SNMP network management station (if configured).

Syntax	`logging history level` To return to the default values, use the `no logging history` command.

Parameters

level	Indicate a value from 0 to 7 or enter one of the following equivalent words: `emergencies`, `alerts`, `critical`, `errors`, `warnings`, `notifications`, `informational`, or `debugging`. The default is **4** or **warnings**.

Defaults	**warnings or 4**
Command Modes	CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information	When you configure the `snmp-server trap-source` command, the system messages logged to the history table are also sent to the SNMP network management station.
Related Commands	show logging — displays information logged to the history buffer.

logging history size

Specify the number of messages stored in the system logging history table.

Syntax	`logging history size size` To return to the default values, use the `no logging history size` command.

Parameters

size	Indicate a value as the number of messages to be stored. The range is from 0 to 500. The default is **1 message**.

Defaults	**1 message**

Command Modes	CONFIGURATION
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	When the number of messages reach the limit you set with the `logging history size` command, older messages are deleted as newer ones are added to the table.
Related Commands	show logging — displays information logged to the history buffer.

logging monitor

Specify which messages are logged to Telnet applications.

Syntax	`logging monitor [level]` To disable logging to terminal connections, use the `no logging monitor` command.
Parameters	*level* — Indicate a value from 0 to 7 or enter one of the following parameters: `emergencies`, `alerts`, `critical`, `errors`, `warnings`, `notifications`, `informational`, or `debugging`. The default is **7** or **debugging**.
Defaults	**7** or **debugging**
Command Modes	CONFIGURATION
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	default logging monitor — returns the logging monitor parameters to the default setting.

logging on

Specify that debug or error messages are asynchronously logged to multiple destinations, such as the logging buffer, Syslog server, or terminal lines.

Syntax	`logging on` To disable logging to logging buffer, Syslog server and terminal lines, use the `no logging on` command.

Defaults	Enabled.
Command Modes	CONFIGURATION
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	When you use the `no logging on` command, messages are logged only to the console.
Related Commands	logging — enables logging to the Syslog server. logging buffered — sets the logging buffered parameters. logging console — sets the logging console parameters. logging monitor — sets the logging parameters for the terminal connections.

logging source-interface

Specify that the IP address of an interface is the source IP address of Syslog packets sent to the Syslog server.

Syntax

```
logging source-interface interface
```

To disable this command and return to the default setting, use the `no logging source-interface` command.

Parameters

interface	Enter the following keywords and slot/port or number information: • For Loopback interfaces, enter the keyword `loopback` then a number from zero (0) to 16383. • For a Port Channel interface, enter the keywords `port-channel` then a number. Tthe range is from 1 to 128. • For a ten-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

Defaults	Not configured.
Command Modes	CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Syslog messages contain the IP address of the interface used to egress the router. By configuring the `logging source-interface` command, the Syslog packets contain the IP address of the interface configured.

Related Commands

logging — enables logging to the Syslog server.

logging synchronous

Synchronize unsolicited messages and output.

Syntax

`logging synchronous [level level | all] [limit number-of-buffers]`

To disable message synchronization, use the `no logging synchronous [level level | all] [limit number-of-buffers]` command.

Parameters

all	Enter the keyword `all` to ensure that all levels are printed asynchronously.
level *level*	Enter the keyword `level` then a number as the severity level. A high number indicates a low severity level and vice versa. The range is from 0 to 7. The default is **2**.
all	Enter the keyword `all` to turn off all.
limit *number-of-buffers*	Enter the keyword `limit` then the number of buffers to be queued for the terminal after which new messages are dropped. The range is from 20 to 300. The default is **20**.

Defaults

Disabled. If enabled without the `level` or `number-of-buffers` options specified, level = **2** and number-of-buffers = **20** are the defaults.

Command Modes

LINE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

When you enable `logging synchronous`, unsolicited messages appear between software prompts and outputs. Only the messages with a severity at or below the set level are sent to the console.

If the message queue limit is reached on a terminal line and messages are discarded, a system message appears on that terminal line. Messages may continue to appear on other terminal lines.

Related Commands	logging on — enables logging.

logging trap

Specify which messages are logged to the Syslog server based the message severity.

Syntax	`logging trap [level]` To return to the default values, use the `default logging trap` command. To disable logging, use the `no logging trap` command.
Parameters	*level* — Indicate a value from 0 to 7 or enter one of the following parameters: `emergencies`, `alerts`, `critical`, `errors`, `warnings`, `notifications`, `informational`, or `debugging`. The default is **6** or **informational**.
Defaults	**6** or **informational**
Command Modes	CONFIGURATION
Command History	Version 8.3.16.1 — Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	logging — enables the logging to another device. logging on — enables logging.

logging version

Displays syslog messages in a RFC 3164 or RFC 5424 format.

Syntax	`logging version {0|1}`
Defaults	`0`
Command Modes	CONFIGURATION
Version 9.5(0.0)	Introduced on the S4810, S4820T, S6000, Z9000, and MXL.
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version 9.5(0.0)	Introduced on the S4810, S4820T, S6000, Z9000, and MXL.

Usage Information

To display syslog messages in a RFC 3164 or RFC 5424 format, use the **log version** command in configuration mode. By default, the system log version is set to **0**.

The following describes the two supported log messages formats:

- `0` – Displays syslog messages format as described in RFC 3164, The BSD syslog Protocol
- `1` – Displays SYSLOG message format as described in RFC 5424, The Syslog Protocol

Example

```
Dell(conf)#logging version ?
<0-1> Select syslog version (default = 0)
Dell(conf)#logging version 1
```

show logging

Display the logging settings and system messages logged to the internal buffer of the switch.

Syntax

```
show logging [number | history [reverse][number] | reverse
[number] | summary]
```

Parameters

number	(OPTIONAL) Enter the number of messages displayed in the output. The range is from 1 to 65535.
history	(OPTIONAL) Enter the keyword `history` to view only information in the Syslog history table.
reverse	(OPTIONAL) Enter the keyword `reverse` to view the Syslog messages in FIFO (first in, first out) order.
summary	(OPTIONAL) Enter the keyword `summary` to view a table showing the number of messages per type and per slot. Slots *7* and *8* represent RPMs.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example (Partial)

```
Dell#show logging
Syslog logging: enabled
  Console logging: level debugging
  Monitor logging: level debugging
  Buffer logging: level debugging, 311 Messages Logged, Size
```

```
(40960 bytes)
  Trap logging: level informational
     Logging to 172.16.1.162
     Logging to 10.10.10.4
     Logging to 10.1.2.4
     Logging to 172.31.1.4
     Logging to 133.33.33.4
May 22 10:21:10: %STKUNIT0-M:CP %SYS-5-CONFIG_I: Configured
from vty0 ( 10.11.68.22 )by admin
May 22 10:16:35: %STKUNIT0-M:CP %SYS-5-CONFIG_I: Configured
from vty0 ( 10.11.68.22 )by admin
May 22 09:39:12: %STKUNIT0-M:CP %SYS-5-CONFIG_I: Configured
from vty0 ( 10.11.68.22 )by admin
May 22 09:03:56: %STKUNIT0-M:CP %SYS-5-CONFIG_I: Configured
from vty0 ( 10.11.68.22 )by admin
May 22 09:01:51: %STKUNIT0-M:CP %SYS-5-CONFIG_I: Configured
from vty0 ( 10.11.68.22 )by admin
May 22 08:53:09: %STKUNIT0-M:CP %SEC-3-
AUTHENTICATION_ENABLE_SUCCESS: Enable password authentication
suc
cess on vty0 ( 10.11.68.22 )
May 22 08:53:04: %STKUNIT0-M:CP %SEC-5-LOGIN_SUCCESS: Login
successful for user admin on vty0
(10.11.68.22)
May 19 16:58:32: %STKUNIT0-M:CP %SEC-5-LOGOUT: Exec session is
terminated for user admin on line vty2
(10.11.68.22)
May 19 14:22:48: %STKUNIT0-M:CP %SYS-5-CONFIG_I: Configured
from vty2 ( 10.11.68.22 )by admin
May 19 12:05:43: %STKUNIT0-M:CP %SYS-5-CONFIG_I: Configured
from vty2 ( 10.11.68.22 )by admin
May 19 10:23:59: %STKUNIT0-M:CP %SYS-5-CONFIG_I: Configured
from vty0 ( 10.11.68.22 )by admin
May 19 10:23:58: %STKUNIT0-M:CP %SEC-5-LOGOUT: Exec
--More--
```

Example (History)

```
Dell#show logging history
Syslog History Table: 1 maximum table entries,
saving level warnings or higher
  SNMP notifications not Enabled
May 22 08:53:09: %STKUNIT0-M:CP %SEC-3-
AUTHENTICATION_ENABLE_SUCCESS: Enable
password authentication success on vty0 ( 10.11.68.22 )
Dell#
```

show logging driverlog stack-unit

Display the driver log for the specified stack member.

Syntax `show logging driverlog stack-unit *unit#*`

Parameters

stack-unit *unit#*	Enter the keywords `stack-unit` then the stack member ID of the switch for which you want to display the driver log. The range is from 0 to 1.

defaults	none
Command Modes	- EXEC - EXEC Privilege
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module..
Usage Information	This command displays internal software driver information, which may be useful during troubleshooting switch initialization errors, such as a downed Port-Pipe.

show logging auditlog

Displays an audit log.

Syntax	`show logging auditlog`
Defaults	none
Command Modes	EXEC
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*. The following is a list of the Dell Networking OS version history for this command. **Version 9.5(0.0)** Introduced on the S4810, S4820T, S6000, Z9000, and MXL.
Example	`Dell(conf)#show logging audit`
Related Commands	clear logging auditlog — clears audit log.

terminal monitor

Configure the system to display messages on the monitor/terminal.

Syntax	`terminal monitor` To return to default settings, use the `terminal no monitor` command.
defaults	Disabled.

Command Modes	- EXEC - EXEC Privilege
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	logging monitor — sets the logging parameters on the monitor/terminal.

51

Stacking

For more information about using the MXL 10/40GbE Switch stacking feature, refer to the *Stacking MXL 10/40GbE Switches* chapter in the *Dell Networking OS Configuration Guide*.

redundancy disable-auto-reboot

Prevent the MXL 10/40GbE switch stack management unit from rebooting if it fail.

Syntax

`redundancy disable-auto-reboot stack-unit [0–5 | members]`

To return to the default, use the `no redundancy disable-auto-reboot stack-unit [0–5 | members]` command.

Defaults

Disabled (the failed switch is automatically rebooted).

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

When the command is given as `redundancy disable-auto-reboot stack-unit`, it prevents the MXL 10/ 40GbE switch stack management unit and standby unit from rebooting if they fail.

When a particular unit number in the range from 0 to 5 is issued as part of the CLI, it prevents that particular unit from rebooting after failure.

When members are issued as part of the CLI, all the units part of the stack are prevented from rebooting after failure.

The unit does not reboot until it is manually rebooted.

Related Commands

show redundancy — displays the current redundancy status.

redundancy force-failover stack-unit

Force the standby unit in the stack to become the management unit.

Syntax	`redundancy force-failover` *`stack-unit`*
Defaults	Not enabled.
Command Modes	EXEC Privilege
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

reset stack-unit

Reset any designated stack member except the management unit (master unit).

Syntax `reset stack-unit` *`0–5 hard`*

Parameters

0–5	Enter the stack member unit identifier of the stack member to reset.
hard	Reset the stack unit if the unit is in a problem state.

Defaults	none
Command Modes	EXEC
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Resetting the management unit is not allowed, and an error message displays if you try to do so. Resetting is a soft reboot, including flushing the forwarding tables.

Starting with the Dell Networking OS version 7.8.1.0, you can run this command directly on the stack standby unit (standby master) to reset the standby. You cannot reset any other unit from the standby unit.

The first two bold lines in the following example show the output of a *not allowed* reset action. The third bold line shows the output of a successful reset action.

Example

```
Dell# show system brief

Stack MAC : 00:1e:c9:f1:00:7b

Reload Type : jump-start [Next boot : normal-reload]

-- Stack Info --
Unit UnitType   Status  ReqTyp        CurTyp       Version
Ports
---------------------------------------------------------------
```

```
---
0    Management online  MXL-10/40GbE  MXL-10/40GbE 9-1-0-853 56
1    Standby    online  MXL-10/40GbE  MXL-10/40GbE 9-1-0-853 56
2    Member     online  MXL-10/40GbE  MXL-10/40GbE 9-1-0-853 56
3    Member     online  MXL-10/40GbE  MXL-10/40GbE 9-1-0-853 56
4    Member     online  MXL-10/40GbE  MXL-10/40GbE 9-1-0-853 56
5    Member     online  MXL-10/40GbE  MXL-10/40GbE 9-1-0-853 56

Dell#reset stack-unit ?
<0-5> Unit number id
Dell#reset stack-unit 0
% Error: Reset of master unit is not allowed.
Dell(standby)#reset stack-unit 3
% Error: Reset of stack units from standby is not allowed.
Dell(standby)#
Dell(standby)#reset stack-unit 1
<00:02:50: %STKUNIT4-S:CP %CHMGR-5-STACKUNIT_RESET: Stack unit
4 being reset
00:02:50: %STKUNIT4-S:CP %CHMGR-2-STACKUNIT_DOWN: Stack unit 4
down - reset
00:02:50: %STKUNIT4-S:CP %IFMGR-1-DEL_PORT: Removed port:
TenGig 4/1-48
Dell#rebooting
U-Boot 1.1.4 (June 6 2012 - 00:00:04)
```

Related Commands

- reload — reboots the system.
- redundancy disable-auto-reboot— resets the designated stack member.

show redundancy

Display the current redundancy configuration (status of automatic reboot configuration on stack management unit).

Syntax

`show redundancy`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show redundancy

-- Stack-unit Status --
------------------------------------------------
  Mgmt ID:                     0
  Stack-unit ID:               0
  Stack-unit Redundancy Role: Primary
  Stack-unit State:            Active
  Stack-unit SW Version:       E8-3-16-160
  Link to Peer:                Down
  Peer Stack-unit:             not present

-- Stack-unit Redundancy Configuration --
```

```
-----------------------------------------------
  Primary Stack-unit:      mgmt-id 0
  Auto Data Sync:          Full
  Failover Type:           Hot Failover
  Auto reboot Stack-unit:  Enabled
  Auto failover limit:     3 times in 60 minutes

-- Stack-unit Failover Record --
-----------------------------------------------
  Failover Count:          0
  Last failover timestamp: None
  Last failover Reason:    None
  Last failover type:      None

-- Last Data Block Sync Record: --
-----------------------------------------------
  Stack Unit Config:  no block sync done
    Start-up Config:  no block sync done
  Runtime Event Log:  no block sync done
     Running Config:  no block sync done
            ACL Mgr:  no block sync done
               LACP:  no block sync done
                STP:  no block sync done
               SPAN:  no block sync done
Dell#
```

Related Commands	redundancy disable-auto-reboot — prevents the system from auto-rebooting if it fails.

show system stack-ports

Display information about the stacking ports on all switches in the MXL 10/40GbE stack.

Syntax `show system stack-ports [status | topology]`

Parameters

status	(OPTIONAL) Enter the keyword `status` to display the command output without the Connection field.
topology	(OPTIONAL) Enter the keyword `topology` to limit the table to just the Interface and Connection fields.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information The following describes the `show interfaces` command shown in the following example.

Field	Description
Topology	Lists the topology of stack ports connected: Ring, Daisy chain, or Standalone.
Interface	The unit/port ID of the connected stack port on this unit.
Link Speed	Link Speed of the stack port (10 or 40) in Gb/s.
Admin Status	The only currently listed status is Up.
Connection	The stack port ID to which this unit’s stack port is connected.

Example

```
Dell# show system stack-ports
Topology: Ring

Interface Connection Link Speed    Admin  Link   Trunk
                     (Gb/s)        Status Status Group
0/33      1/37       40            up       up
0/37      2/33       40            up       up
0/41      1/49       40            up       up
0/45      2/53       40            up       up
1/33      2/37       40            up       up
1/37      0/33       40            up       up
1/49      0/41       40            up       up
1/53      2/49       40            up       up
2/33      0/37       40            up       up
2/37      1/33       40            up       up
2/49      1/53       40            up       up
2/53      0/45       40            up       up
```

Example (Status)

```
Dell# show system stack-ports status
Topology: Ring
Interface Link Speed   Admin  Link   Trunk
          (Gb/s)       Status Status Group
0/33      40           up     up
0/37      40           up     up
0/41      40           up     up
0/45      40           up     up
1/33      40           up     up
1/37      40           up     up
1/49      40           up     up
1/53      40           up     up
2/33      40           up     up
2/37      40           up     up
2/49      40           up     up
2/53      40           up     up
```

Example (Topology)

```
Dell# show system stack-ports
Topology: Ring

Interface Connection Trunk
                     Group
0/33      1/37
0/37      2/33
0/41      1/49
0/45      2/53
1/33      2/37
1/37      0/33
1/49      0/41
```

```
1/53      2/49
2/33      0/37
2/37      1/33
2/49      1/53
2/53      0/45
```

Related Commands

- redundancy disable-auto-reboot — resets the designated stack member.
- show hardware stack-unit — displays the data plane or management plane input and output statistics of the designated component of the designated stack member.
- show system — displays the current status of all stack members or a specific member.

show system stack-unit stack-group

Display the stack-groups present/configured for a MXL 10/40GbE switch stack unit.

Syntax `show system stack-unit unit-number stack-group [configured]`

Parameters

unit number <0–5>	Number of the member stack unit. The valid values are from 0 to 5. The default is **0**.

Command Modes EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

- reload — reboots the system.
- show system — displays the current status of all stack members or a specific member.

stack-unit stack-group

Configure a 40GbE port for stacking mode.

Syntax `stack-unit unit number stack-group group number`

Parameters

unit number <0–5>	Number of the member stack unit. The valid values are from 0 to 5.
group number <0–5>	Number of the stacked port on the unit. The valid values are from 0 to 5.

Command Modes	CONFIGURATION
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	- reload — reboots the system. - show system — displays the current status of all stack members or a specific member. - show system stack-unit stack-group displays the stack-groups present/configured for a MXL 10/40GbE switch stack unit

stack-unit priority

Configure the ability of an MXL 10/40GbE switch to become the management unit of a stack.

Syntax

```
stack-unit 0–5 priority 1–14
```

Parameters

0–5	Enter the stack member unit identifier, from 0 to 5, of the switch on which you want to set the management priority.
1–14	This preference parameter allows you to specify the management priority of one backup switch over another, with 1 the lowest priority and 14 the highest. The switch with the highest priority value will be chosen to become the management unit.

Defaults	0
Command Modes	CONFIGURATION
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	- reload — reboots the system. - show system — displays the status of all stack members or a specific member.

stack-unit provision

Preconfigure a logical stacking ID of a switch that joins the stack. This is an optional command that is executed on the management unit.

Syntax

```
stack-unit 0–5] provision {MXL-10/40GbE}
```

Parameters

0–5	Enter a stack member identifier, from 0 to 5, of the switch that you want to add to the stack.
MXL-10/40GbE	Enter the model identifier of the switch to be added as a stack member. This identifier is also referred to as the *provision type*.

Command Modes CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

- reload — reboots the system.
- show system — displays the status of all stack members or a specific member.

stack-unit renumber

Change the stack member ID of any stack member or a stand-alone unit.

Syntax

```
stack-unit 0-5 renumber 0-11
```

Parameters

0-5	The first instance of this value is the stack member unit identifier, from 0 to 5, of the switch that you want add to the stack. The second instance of this value is the desired new unit identifier number.

Defaults none

Command Modes EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

You can renumber any switch, including the management unit or a stand-alone unit.

You cannot renumber a unit to a number of an active member in the stack.

When executing this command on the master, the stack reloads. When the members are renumbered, only that specific unit is reset and comes up with the new unit number.

Example

```
Dell#stack-unit 0 renumber 2

Renumbering master unit will reload the stack. Proceed to
renumber [confirm yes/
no]:
```

Related Commands

- reload — reboots the system.
- redundancy disable-auto-reboot — resets the designated stack member.
- show system — displays the current status of all stack members or a specific member.

52

Storm Control

The Dell Networking Operating System (OS) storm control feature allows you to limit or suppress traffic during a traffic storm.

Storm control is supported on the Dell Networking OS Z-Series S4810 S4820T platforms.

Important Points to Remember

- Interface commands can only be applied on physical interfaces (virtual local area networks [VLANs] and link aggregation group [LAG] interfaces are not supported).
- An INTERFACE-level command only supports storm control configuration on ingress.
- An INTERFACE-level command overrides any CONFIGURATION-level ingress command for that physical interface, if both are configured.
- Do not apply per-VLAN quality of service (QoS) on an interface that has storm control enabled (either on an interface or globally).

show storm-control broadcast

Display the storm control broadcast configuration.

Syntax `show storm-control broadcast [interface]`

Parameters

interface	(OPTIONAL) Enter one of the following interfaces to display the interface-specific storm control configuration: • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/ port information.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show storm-control broadcast tengigabitethernet 3/24

  Broadcast storm control configuration

Interface    Direction  Packets/Second
----------------------------------------
TenGig 3/24  Ingress    1000
Dell#
```

show storm-control multicast

Display the storm control multicast configuration.

Syntax `show storm-control multicast [`*`interface`*`]`

Parameters

interface	(OPTIONAL) Enter one of the following interfaces to display the interface specific storm control configuration: • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/ port information.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show storm-control multicast gigabitethernet 1/0

Multicast storm control configuration

Interface  Direction     Packets/Second
-----------------------------------------
Gi 1/0     Ingress       5

Dell#
```

show storm-control unknown-unicast

Display the storm control unknown-unicast configuration.

Syntax `show storm-control unknown-unicast [`*`interface`*`]`

Parameters		
	interface	(OPTIONAL) Enter one of the following interfaces to display the interface specific storm control configuration: • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/ port information.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on MXL 10/40GbE Switch IO Module

Example

```
Dell#show storm-control unknown-unicast tengigabitethernet 3/0

Unknown-unicast storm control configuration

Interface   Direction  Packets/Second
----------------------------------------
TenGig 3/0  Ingress    1000

Dell#
```

storm-control broadcast (Configuration)

Configure the percentage of broadcast traffic allowed in the network.

Syntax `storm-control broadcast [packets_per_second in]`

To disable broadcast rate-limiting, use the `no storm-control broadcast [packets_per_second in]` command.

Parameters

packets_per_second	Enter the packets per second of broadcast traffic allowed into the network. The range is from 0 to 33554368.

Defaults none

Command Modes CONFIGURATION (conf)

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information Broadcast storm control is valid on Layer 2/Layer 3 interfaces only. Layer 2 broadcast traffic is treated as unknown-unicast traffic.

storm-control broadcast (Interface)

Configure the percentage of broadcast traffic allowed on an interface.

Syntax	`storm-control broadcast [packets_per_second in]` To disable broadcast storm control on the interface, use the `no storm-control broadcast [packets_per_second in]` command.
Parameters	***packets_per_second*** Enter the packets per second of broadcast traffic allowed into the network. The range is from 0 to 33554368.
Defaults	none
Command Modes	INTERFACE (conf-if-*interface-slot/port*)
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

storm-control multicast (Configuration)

Configure the packets per second (pps) of multicast traffic.

Syntax	`storm-control multicast packets_per_second in` To disable storm-control for multicast traffic into the network, use the `no storm-control multicast packets_per_second in` command.
Parameters	***packets_per_second*** Enter the packets per second of multicast traffic allowed into the network. The range is from 0 to 33554368.
Defaults	none
Command Modes	CONFIGURATION (conf)
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	Broadcast traffic (all 0xFs) should be counted against the broadcast storm control meter, not against the multicast storm control meter. It is possible, however, that some multicast control traffic may get dropped when storm control thresholds are exceeded.

storm-control multicast (Interface)

Configure the percentage of multicast traffic allowed on an MXL switch interface (ingress only).

Syntax

`storm-control multicast packets_per_second in`

To disable multicast storm control on the interface, use the `no storm-control multicast packets_per_second in` command.

Parameters

packets_per_second	Enter the packets per second of broadcast traffic allowed into the network. The range is from 0 to 33554368.

Defaults

none

Command Modes

INTERFACE (conf-if-*interface-slot/port*)

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

storm-control unknown-unicast (Configuration)

Configure the percentage of unknown-unicast traffic allowed on an MXL switch (ingress rate only).

Syntax

`storm-control unknown-unicast [packets_per_second in]`

To disable storm control for unknown-unicast traffic, use the `no storm-control unknown-unicast [packets_per_second in]` command.

Parameters

packets_per_second	Enter the packets per second of broadcast traffic allowed into the network. The range is from 0 to 33554368.

Defaults

none

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Unknown Unicast Storm-Control is valid for Layer 2 and Layer 2/Layer 3 interfaces.

storm-control unknown-unicast (Interface)

Configure percentage of unknown-unicast traffic allowed on an MXL switch interface (ingress only).

Syntax	`storm-control unknown-unicast [`*`packets_per_second`*` in]` To disable unknown-unicast storm control on the interface, use the `no storm-control unknown-unicast [`*`packets_per_second`*` in]` command.
Parameters	
packets_per_second	Enter the packets per second of broadcast traffic allowed into the network. The range is from 0 to 33554431.
Defaults	none
Command Modes	INTERFACE (conf-if-*interface-slot/port*)
Command History	
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

53

Spanning Tree Protocol (STP)

The commands in this chapter configure and monitor the IEEE 802.1d spanning tree protocol (STP).

bridge-priority

Set the bridge priority of the switch in an IEEE 802.1D spanning tree.

Syntax

```
bridge-priority {priority-value | primary | secondary}
```

To return to the default value, use the `no bridge-priority` command.

Parameters

priority-value	Enter a number as the bridge priority value. The range is from 0 to 65535. The default is **32768**.
primary	Enter the keyword `primary` to designate the bridge as the root bridge.
secondary	Enter the keyword `secondary` to designate the bridge as a secondary root bridge.

Defaults priority-value = **32768**

Command Modes SPANNING TREE (The prompt is “config-stp”.)

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

debug spanning-tree

Enable debugging of the spanning tree protocol and view information on the protocol.

Syntax

```
debug spanning-tree {stp-id [all | bpdu | events | exceptions]
| protocol}
```

To disable debugging, use the `no debug spanning-tree` command.

Parameters

stp-id	Enter zero (0). The switch supports one spanning tree group with a group ID of 0.

protocol	Enter the keyword for the type of STP to debug, either `mstp`, `pvst`, or `rstp`.
all	(OPTIONAL) Enter the keyword `all` to debug all spanning tree operations.
bpdu	(OPTIONAL) Enter the keyword `bpdu` to debug bridge protocol data units.
events	(OPTIONAL) Enter the keyword `events` to debug STP events.

Command Modes

EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

When you enable `debug spanning-tree bpdu` for multiple interfaces, the software only sends information on BPDUs for the last interface specified.

Related Commands

portfast bpdufilter default — enters SPANNING TREE mode on the switch.

description

Enter a description of the spanning tree.

Syntax

`description {`*`description`*`}`

To remove the description from the spanning tree, use the `no description {`*`description`*`}` command.

Parameters

description	Enter a description to identify the spanning tree (80 characters maximum).

Defaults

none

Command Modes

SPANNING TREE (The prompt is “config-stp”.)

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

portfast bpdufilter default — enters SPANNING TREE mode on the switch.

disable

Disable the spanning tree protocol globally on the switch.

Syntax	`disable` To enable Spanning Tree Protocol, use the `no disable` command.
Defaults	Enabled (that is, the spanning tree protocol is disabled.)
Command Modes	SPANNING TREE
Command History	**Version 8.3.16.1** — Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	portfast bpdufilter default — enters SPANNING TREE mode.

forward-delay

The amount of time the interface waits in the Listening state and the Learning state before transitioning to the Forwarding state.

Syntax	`forward-delay` *`seconds`* To return to the default setting, use the `no forward-delay` command.
Parameters	*seconds* — Enter the number of seconds that the system waits before transitioning STP to the Forwarding state. The range is from 4 to 30. The default is **15 seconds**.
Defaults	**15 seconds**
Command Modes	SPANNING TREE
Command History	**Version 8.3.16.1** — Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	max-age — changes the wait time before STP refreshes protocol configuration information. hello-time — changes the time interval between BPDUs.

hello-time

Set the time interval between generation of the spanning tree bridge protocol data units (BPDUs).

Syntax

```
hello-time seconds
```

To return to the default value, use the `no hello-time` command.

Parameters

seconds	Enter a number as the time interval between transmission of BPDUs. The range is from 1 to 10. The default is **2 seconds**.

Defaults

2 seconds

Command Modes

SPANNING TREE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

`forward-delay` — changes the wait time before STP transitions to the Forwarding state.

`max-age` — changes the wait time before STP refreshes protocol configuration information.

max-age

To maintain configuration information before refreshing that information, set the time interval for the spanning tree bridge.

Syntax

```
max-age seconds
```

To return to the default values, use the `no max-age` command.

Parameters

seconds	Enter a number of seconds the system waits before refreshing configuration information. The range is from 6 to 40. The default is **20 seconds**.

Defaults

20 seconds

Command Modes

SPANNING TREE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

`forward-delay` — changes the wait time before STP transitions to the Forwarding state.

hello-time — changes the time interval between BPDUs.

portfast bpdufilter default

Enable BPDU Filter globally to filter transmission of BPDU on port fast enabled interfaces.

Syntax `portfast bpdufilter default`

To disable global bpdu filter default, use the `no edge-port bpdufilter default` command.

Defaults Disabled

Command Modes SPANNING TREE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

protocol spanning-tree

To enable and configure the spanning tree group, enter SPANNING TREE mode.

Syntax `protocol spanning-tree` *`stp-id`*

To disable the Spanning Tree group, use the `no protocol spanning-tree` *`stp-id`* command.

Parameters

stp-id	Enter zero (0). The system supports one spanning tree group, group 0.

Defaults Not configured.

Command Modes CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information STP is not enabled when you enter SPANNING TREE mode. To enable STP globally on the switch, use the `no disable` command from SPANNING TREE mode.

Example

```
Dell(conf)#protocol spanning-tree 0
Dell(config-stp)#
```

Related Commands disable — disables spanning tree group 0. To enable spanning tree group 0, use the `no disable` command.

show config

Display the current configuration for the mode. Only non-default values display.

Syntax	`show config`
Command Modes	SPANNING TREE
Command History	Version 8.3.16.1 — Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell(config-stp)#show config
protocol spanning-tree 0
  no disable
Dell(config-stp)#
```

show spanning-tree 0

Display the spanning tree group configuration and status of interfaces in the spanning tree group.

Syntax

```
show spanning-tree 0 [active | brief | guard | interface
interface | root | summary]
```

Parameters

0	Enter `0` (zero) to display information about that specific spanning tree group.
active	(OPTIONAL) Enter the keyword `active` to display only active interfaces in spanning tree group 0.
brief	(OPTIONAL) Enter the keyword `brief` to display a synopsis of the spanning tree group configuration information.
guard	(OPTIONAL) Enter the keyword `guard` to display the type of guard enabled on an STP interface and the current port state.
interface *interface*	(OPTIONAL) Enter the keyword `interface` and the type slot/port of the interface you want displayed. Type slot/port options are the following: • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
root	(OPTIONAL) Enter the keyword `root` to display configuration information on the spanning tree group root.
summary	(OPTIONAL) Enter the keyword `summary` to only the number of ports in the spanning tree group and their state.

Command Modes

EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Enable spanning tree group 0 prior to using this command.

The following describes the `show spanning-tree 0` command shown in the example.

Field	Description
"Bridge Identifier..."	Lists the bridge priority and the MAC address for this STP bridge.
"Configured hello..."	Displays the settings for hello time, max age, and forward delay.
"We are..."	States whether this bridge is the root bridge for the STG.
"Current root..."	Lists the bridge priority and MAC address for the root bridge.
"Topology flag..."	States whether the topology flag and the detected flag were set.
"Number of..."	Displays the number of topology changes, the time of the last topology change, and on what interface the topology change occurred.
"Timers"	Lists the values for the following bridge timers: hold time, topology change, hello time, max age, and forward delay.
"Times"	List the number of seconds since the last: • hello time • topology change • notification • aging
"Port 1..."	Displays the Interface type slot/port information and the status of the interface (Disabled or Enabled).
"Port path..."	Displays the path cost, priority, and identifier for the interface.
"Designated root..."	Displays the priority and MAC address of the root bridge of the STG that the interface belongs.
"Designated port..."	Displays the designated port ID.

Example

```
Dell#show spann 0

Executing IEEE compatible Spanning Tree Protocol
 Bridge Identifier has priority 32768, Address 0001.e800.0a56
 Configured hello time 2, max age 20, forward delay 15
 We are the root of the spanning tree
 Current root has priority 32768 address 0001.e800.0a56
 Topology change flag set, detected flag set
 Number of topology changes 1 last change occurred 0:00:05 ago
   from GigabitEthernet 1/3
 Timers:hold 1, topology change 35
        hello 2, max age 20, forward_delay 15
 Times:hello 1, topology change 1, notification 0, aging 2

Port 26 (GigabitEthernet 1/1) is Forwarding
 Port path cost 4, Port priority 8, Port Identifier 8.26
 Designated root has priority 32768, address 0001.e800.0a56
 Designated bridge has priority 32768, address 0001.e800.0a56
 Designated port id is 8.26, designated path cost 0
 Timers: message age 0, forward_delay 0, hold 0
 Number of transitions to forwarding state 1
 BPDU: sent:18, received 0
 The port is not in the portfast mode

Port 27 (GigabitEthernet 1/2) is Forwarding
 Port path cost 4, Port priority 8, Port Identifier 8.27
 Designated root has priority 32768, address 0001.e800.0a56
 Designated bridge has priority 32768, address 0001.e800.0a56
 Designated port id is 8.27, designated path cost 0
 Timers: message age 0, forward_delay 0, hold 0
 Number of transitions to forwarding state 1
 BPDU: sent:18, received 0
 The port is not in the portfast mode

Port 28 (GigabitEthernet 1/3) is Forwarding
 Port path cost 4, Port priority 8, Port Identifier 8.28
 Designated root has priority 32768, address 0001.e800.0a56
 Designated bridge has priority 32768, address 0001.e800.0a56
 Designated port id is 8.28, designated path cost 0
 Timers: message age 0, forward_delay 0, hold 0
 Number of transitions to forwarding state 1
 BPDU: sent:31, received 0
 The port is not in the portfast mode

Dell#
```

Example (Brief)

```
Dell#show span 0 brief
  Executing IEEE compatible Spanning Tree Protocol
    Root ID Priority 32768
      Address 0001.e800.0a56
    Root Bridge hello time 2, max age 20, forward delay 15
    Bridge ID Priority 32768,
      Address 0001.e800.0a56
    Configured hello time 2, max age 20, forward delay 15
Interface                        Designated
Name   PortID Prio Cost Sts Cost Bridge ID            PortID
-------------- ------ ---- ---- --- ----- ------------------
Gi 1/1 8.26   8   4     FWD 0    32768 0001.e800.0a56 8.26
Gi 1/2 8.27   8   4     FWD 0    32768 0001.e800.0a56 8.27
Gi 1/3 8.28   8   4     FWD 0    32768 0001.e800.0a56 8.28
Dell#
```

Usage Information

The following describes the `show spanning-tree 0 guard` command shown in the example.

Field	Description
Interface Name	STP interface.

Field	Description
Instance	STP 0 instance.
Sts	Port state: root-inconsistent (INCON Root), forwarding (FWD), listening (LIS), blocking (BLK), or shut down (EDS Shut).
Guard Type	Type of STP guard configured (Root, Loop, or BPDU guard).
Bpdu Filter	BPDU Filter enabled - Yes, BPDU Filter disabled - No

Example (Guard)

```
Dell#show spanning-tree 0 guard
Interface
Name   Instance Sts           Guard type
--------- -------- --------- ----------
Gi 0/1 0        INCON(Root)  Rootguard
Gi 0/2 0        LIS          Loopguard
Gi 0/3 0        EDS (Shut)   Bpduguard
```

spanning-tree 0

Assigns a Layer 2 interface to STP instance 0 and configures a port cost or port priority, or enables loop guard, root guard, or the Portfast feature on the interface.

Syntax

`spanning-tree` *`stp-id`* `{cost` *`cost`* `| {rootguard} | portfast [bpduguard [shutdown-on-violation]| bpdufilter] | priority` *`priority`*`}`

To disable Spanning Tree group on an interface, use the `no spanning-tree` *`stp-id`* `{cost` *`cost`* `| {rootguard} | portfast [bpduguard [shutdown-on-violation] | bpdufilter] | priority` *`priority`*`}` command.

Parameters

stp-id	Enter the STP instance ID. The range is 0.
cost *cost*	Enter the keyword `cost` then a number as the cost. The range is 1 to 65535. The defaults are: • 40-Gigabit Ethernet interface = **1**. • 10-Gigabit Ethernet interface = **2**. • Port Channel interface with 40-Gigabit Ethernet = **1**. • Port Channel interface with 10-Gigabit Ethernet = **1**.
rootguard	Enter the keyword `rootguard` to enable STP root guard on a port or port-channel interface.

portfast [bpduguard [shutdown-on-viol ation] | bpdufilter]	Enter the keyword `portfast` to enable Portfast to move the interface into Forwarding mode immediately after the root fails. Enter the optional keyword `bpduguard` to disable the port when it receives a BPDU. Enter the optional keywords `shutdown-on-violation` to hardware disable an interface when a BPDU is received and the port is disabled. Enter the keyword `bpdufilter` to enable on an interface; it should stop sending and receiving BPDUs on the port fast enabled ports.
priority *priority*	Enter keyword `priority` then a number as the priority. The range is zero (0) to 15. The default is **8**.

Defaults cost = depends on the interface type; priority = **8**

Command Modes INTERFACE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module..

Usage Information

If you enable `portfast bpduguard` on an interface and the interface receives a BPDU, the software disables the interface and sends a message stating that fact. The port is in ERR_DISABLE mode, yet appears in the `show interface` commands as enabled. If you do not enable `shutdown-on-violation`, BPDUs still are sent to the RPM CPU.

STP root guard is supported on a port or port-channel enabled in any Spanning Tree mode: Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), Multiple Spanning Tree Protocol (MSTP), and Per-VLAN Spanning Tree Plus (PVST +).

Root guard is supported on any STP-enabled port or port-channel except when used as a stacking port. When enabled on a port, root guard applies to all VLANs configured on the port.

54

System Time and Date

The commands in this chapter configure time values on the system, either using the Dell Networking Operating System (OS), or the hardware, or using the network time protocol (NTP). With NTP, the switch can act only as a client to an NTP clock host.

For more information, refer to the “Network Time Protocol” section of the *Management* chapter in the *Dell Networking OS Configuration Guide*.

calendar set

Set the time and date for the switch hardware clock.

Syntax

```
calendar set time month day year
```

Parameters

time	Enter the time in hours:minutes:seconds. For the hour variable, use the 24-hour format; for example, 17:15:00 is 5:15 pm.
month	Enter the name of one of the 12 months in English. You can enter the name of a day to change the order of the display to time day month year.
day	Enter the number of the day. The range is from 1 to 31. You can enter the name of a month to change the order of the display to time day month year.
year	Enter a four-digit number as the year. The range is from 1993 to 2035.

Command Modes

EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

You can change the order of the month and day parameters to enter the time and date as time day month year.

In the switch, the hardware clock is separate from the software and is called the calendar. This hardware clock runs continuously. After the hardware clock (the calendar) is set, the system automatically updates the software clock after system bootup. You cannot delete the hardware clock (calendar).

To manually update the software with the hardware clock, use the `clock read-calendar` command.

Example

```
Dell#calendar set 12:11:00 21 may 2012
Dell#
```

Related Commands

clock read-calendar — sets the software clock based on the hardware clock.

clock set — sets the software clock.

clock update-calendar — sets the hardware clock based on the software clock.

show clock — displays the clock settings.

clock read-calendar

Set the software clock on the switch from the information set in hardware clock (calendar).

Syntax `clock read-calendar`

Defaults Not configured.

Command Modes EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

In the switch, the hardware clock is separate from the software and is called the calendar. This hardware clock runs continuously. After the hardware clock (the calendar) is set, the system automatically updates the software clock after system bootup.

You cannot delete this command (there is not a `no` version of this command).

clock set

Set the software clock in the switch.

Syntax `clock set` *`time month day year`*

Parameters

time	Enter the time in hours:minutes:seconds. For the hour variable, use the 24-hour format; example, 17:15:00 is 5:15 pm.

month	Enter the name of one of the 12 months, in English. You can enter the number of a day and change the order of the display to time day month year.
day	Enter the number of the day. The range is from 1 to 31. You can enter the name of a month to change the order of the display to time month day year.
year	Enter a four-digit number as the year. The range is from 1993 to 2035.

Defaults

Not configured.

Command Modes

EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

You can change the order of the `month` and `day` parameters to enter the time and date as time day month year. You cannot delete the software clock.

The software clock runs only when the software is up. The clock restarts, based on the hardware clock, when the switch reboots.

Dell Networking OS recommends using an outside time source, such as NTP, to ensure accurate time on the switch.

Example

```
Dell#clock set 12:11:00 21 may 2012
Dell#
```

Related Commands

ntp update-calendar — sets the switch using the NTP settings.

clock summer-time date

Set a date (and time zone) on which to convert the switch to daylight saving time on a one-time basis.

Syntax

```
clock summer-time time-zone date start-month start-day start-year start-time end-month end-day end-year end-time [offset]
```

To delete a daylight saving time zone configuration, use the `no clock summer-time` command.

Parameters

time-zone	Enter the three-letter name for the time zone. This name is displayed in the show clock output.
start-month	Enter the name of one of the 12 months in English. You can enter the name of a day to change the order of the display to time day month year.

start-day	Enter the number of the day. The range is from 1 to 31. You can enter the name of a month to change the order of the display to time day month year.
start-year	Enter a four-digit number as the year. The range is from 1993 to 2035.
start-time	Enter the time in hours:minutes. For the hour variable, use the 24-hour format; example, 17:15 is 5:15 pm.
end-day	Enter the number of the day. The range is from 1 to 31. You can enter the name of a month to change the order of the display to time day month year.
end-month	Enter the name of one of the 12 months in English. You can enter the name of a day to change the order of the display to time day month year.
end-time	Enter the time in hours:minutes. For the hour variable, use the 24-hour format; example, 17:15 is 5:15 pm.
end-year	Enter a four-digit number as the year. The range is from 1993 to 2035.
offset	(OPTIONAL) Enter the number of minutes to add during the summer-time period. The range is from 1 to1440. The default is **60 minutes**.

Defaults — Not configured.

Command Modes — CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

calendar set — sets the hardware clock.

clock summer-time recurring — sets a date (and time zone) on which to convert the switch to daylight saving time each year.

show clock — displays the current clock settings.

clock summer-time recurring

Set the software clock to convert to daylight saving time on a specific day each year.

Syntax

```
clock summer-time time-zone recurring [start-week start-day
start-month start-time end-week end-day end-month end-time
[offset]]
```

To delete a daylight saving time zone configuration, use the `no clock summer-time` command.

Parameters

time-zone	Enter the three-letter name for the time zone. This name is displayed in the show clock output. You can enter up to eight characters.
start-week	(OPTIONAL) Enter one of the following as the week that daylight saving begins and then enter values for start-day through end-time: • `week-number`: Enter a number from 1 to 4 as the number of the week in the month to start daylight saving time. • `first`: Enter this keyword to start daylight saving time in the first week of the month. • `last`: Enter this keyword to start daylight saving time in the last week of the month.
start-day	Enter the name of the day that you want daylight saving time to begin. Use English three letter abbreviations; for example, Sun, Sat, Mon, and so on. The range is from Sun to Sat.
start-month	Enter the name of one of the 12 months in English.
start-time	Enter the time in hours:minutes. For the hour variable, use the 24-hour format; example, 17:15 is 5:15 pm.
end-week	Enter the one of the following as the week that daylight saving ends: • `week-number`: enter a number from 1 to 4 as the number of the week to end daylight saving time. • `first`: enter the keyword `first` to end daylight saving time in the first week of the month. • `last`: enter the keyword `last` to end daylight saving time in the last week of the month.
end-day	Enter the weekday name that you want daylight saving time to end. Enter the weekdays using the three letter abbreviations; for example Sun, Sat, Mon, and so on. The range is from Sun to Sat.
end-month	Enter the name of one of the 12 months in English.
end-time	Enter the time in hours:minutes:seconds. For the hour variable, use the 24-hour format; example, 17:15:00 is 5:15 pm.
offset	(OPTIONAL) Enter the number of minutes to add during the summer-time period. The range is from 1 to 1440. The default is **60 minutes**.

Defaults Not configured.

Command Modes CONFIGURATION

Command History	**Version 8.3.16.1**	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

calendar set — sets the hardware clock.

clock summer-time date — sets a date (and time zone) on which to convert the switch to daylight saving time on a one-time basis.

show clock — displays the current clock settings.

clock timezone

Configure a timezone for the switch.

Syntax

```
clock timezone timezone-name offset
```

To delete a timezone configuration, use the `no clock timezone` command.

Parameters

timezone-name	Enter the name of the timezone. You cannot use spaces.
offset	Enter one of the following: • a number from 1 to 23 as the number of hours in addition to universal time coordinated (UTC) for the timezone. • a minus sign (-) then a number from 1 to 23 as the number of hours.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History	**Version 8.3.16.1**	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Coordinated universal time (UTC) is the time standard based on the International Atomic Time standard, commonly known as Greenwich Mean time. When determining system time, include the differentiator between UTC and your local timezone. For example, San Jose, CA is the Pacific Timezone with a UTC offset of -8.

clock update-calendar

Set the switch hardware clock based on the software clock.

Syntax	`clock update-calendar`
Defaults	Not configured.
Command Modes	EXEC Privilege
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	Use this command only if you are sure that the hardware clock is inaccurate and the software clock is correct. You cannot delete this command (there is not a `no` form of this command).
Related Commands	calendar set — sets the hardware clock.

debug ntp

Display network time protocol (NTP) transactions and protocol messages for troubleshooting.

Syntax	`debug ntp {adjust | all | authentication | events | loopfilter | packets | select | sync}` To disable debugging of NTP transactions, use the `no debug ntp {adjust | all | authentication | events | loopfilter | packets | select | sync}` command.

Parameters

adjust	Enter the keyword `adjust` to display information on NTP clock adjustments.
all	Enter the keyword `all` to display information on all NTP transactions.
authentication	Enter the keyword `authentication` to display information on NTP authentication transactions.
events	Enter the keyword `events` to display information on NTP events.
loopfilter	Enter the keyword `loopfilter` to display information on NTP local clock frequency.
packets	Enter the keyword `packets` to display information on NTP packets.
select	Enter the keyword `select` to display information on the NTP clock selection.

sync	Enter the keyword `sync` to display information on the NTP clock synchronization.

Command Modes

EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

ntp authenticate

Enable authentication of NTP traffic between the switch and the NTP time serving hosts.

Syntax

```
ntp authenticate
```

To disable NTP authentication, use the `no ntp authentication` command.

Defaults

Not enabled.

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

You also must configure an authentication key for NTP traffic using the `ntp authentication-key` command.

Related Commands

ntp authentication-key — configures the authentication key for NTP traffic.

ntp trusted-key — configures a key to authenticate.

ntp authentication-key

Specify a key for authenticating the NTP server.

Syntax

```
ntp authentication-key number md5 [0 | 7] key
```

Parameters

number	Specify a number for the authentication key. The range is from 1 to 4294967295. This number must be the same as the `number` parameter configured in the `ntp trusted-key` command.
md5	Specify that the authentication key is encrypted using MD5 encryption algorithm.

0	Specify that authentication key is entered in an unencrypted format (default).
7	Specify that the authentication key is entered in DES encrypted format.
key	Enter the authentication key in the previously specified format.

Defaults

NTP authentication is not configured by default. If you do not specify the option [`0` | `7`], **0** is selected by default.

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

After configuring the `ntp authentication-key` command, configure the `ntp trusted-key` command to complete NTP authentication.

The Dell Networking OS versions 8.2.1.0 and later use an encryption algorithm to store the authentication key that is different from previous versions; beginning in version 8.2.1.0, the system uses DES encryption to store the key in the startup-config when you enter the `ntp authentication-key` command. Therefore, if your system boots with a startup-configuration from an versions prior to 8.2.1.0 in which you have configured `ntp authentication-key`, the system cannot correctly decrypt the key, and cannot authenticate NTP packets. In this case you must re-enter this command and save the running-config to the startup-config.

Related Commands

ntp authenticate — enables NTP authentication.

ntp trusted-key — configures a trusted key.

ntp broadcast client

Set up the interface to receive NTP broadcasts from an NTP server.

Syntax

`ntp broadcast client`

To disable broadcast, use the `no ntp broadcast client` command.

Defaults

Disabled.

Command Modes

INTERFACE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

ntp disable

Prevent an interface from receiving NTP packets.

Syntax	`ntp disable` To re-enable NTP on an interface, use the `no ntp disable` command.
Defaults	Disabled (that is, if you configure an NTP host, all interfaces receive NTP packets)
Command Modes	INTERFACE
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

ntp multicast client

To receive NTP information from the network via multicast, configure the switch.

Syntax

`ntp multicast client [multicast-address]`

To disable multicast reception, use the `no ntp multicast client [multicast-address]` command.

Parameters

multicast-address	(OPTIONAL) Enter a multicast address. Enter either an IPv4 address in dotted decimal format. If you do not enter a multicast address, the address 224.0.1.1 is configured if the interface address is IPv4.

Defaults	Not configured.
Command Modes	INTERFACE
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

ntp server

Configure an NTP time-serving host.

Syntax

`ntp server {hostname | ipv4-address} [key keyid] [prefer] [version number]`

Parameters

ipv4-address	Enter an IPv4 address (A.B.C.D).

hostname	Enter the hostname of the server.
key *keyid*	(OPTIONAL) Enter the keyword `key` and a number as the NTP peer key. The range is from 1 to 4294967295.
prefer	(OPTIONAL) Enter the keyword `prefer` to indicate that this peer has priority over other servers.
version *number*	(OPTIONAL) Enter the keyword `version` and a number to correspond to the NTP version used on the server. The range is from 1 to 3.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

Version 8.3.11.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

You can configure multiple time-serving hosts (up to 250). From these time-serving hosts, the system chooses one NTP host with which to synchronize. To determine which server was selected, use the `show ntp associations` command.

Because many polls to NTP hosts can impact network performance, Dell Networking OS recommends limiting the number of hosts configured.

Related Commands

show ntp associations — displays the NTP servers configured and their status.

ntp source

Specify an interface's IP address to be included in the NTP packets.

Syntax

`ntp source` *`interface`*

To delete the configuration, use the `no ntp source` command.

Parameters

interface	Enter the following keywords and slot/port or number information: • For Loopback interfaces, enter the keyword `loopback` then a number from zero (0) to 16383. • For a Port Channel interface, enter the keyword `lag` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

- For VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

Defaults	Not configured.
Command Modes	CONFIGURATION
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

ntp trusted-key

Set a key to authenticate the system to which NTP synchronizes.

Syntax

`ntp trusted-key` *`number`*

To delete the key, use the `no ntp trusted-key` *`number`* command.

Parameters

number	Enter a number as the trusted key ID. The range is from 1 to 4294967295.

Defaults	Not configured.
Command Modes	CONFIGURATION
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The `number` parameter in the `ntp trusted-key` command must be the same number as the `number` parameter in the `ntp authentication-key` command. If you change the `ntp authentication-key` command, you must also change the `ntp trusted-key` command.

Related Commands

ntp authentication-key — sets an authentication key for NTP.

ntp authenticate — enables the NTP authentication parameters you set.

ntp update-calendar

Configure the system to update the calendar (the hardware clock) with the NTP-derived time.

Syntax

`ntp update-calendar [`*`minutes`*`]`

To return to default setting, use the `no ntp update-calendar` command.

Parameters	*minutes*	(OPTIONAL) Enter the number of minutes between updates from NTP to the hardware clock. The range is from 1 to 1440. The default is **60 minutes**.

Defaults: Not enabled.

Command Modes: CONFIGURATION

Command History	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

show calendar

Display the current date and time based on the switch hardware clock.

Syntax: `show calendar`

Command Modes:

- EXEC
- EXEC Privilege

Command History	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show calendar
12:29:34 pacific Tue May 22 2012
Dell#
```

Related Commands: show clock — displays the time and date from the switch software clock.

show clock

Display the current clock settings.

Syntax: `show clock [detail]`

Parameters	detail	(OPTIONAL) Enter the keyword `detail` to view the source information of the clock.

Command Modes:

- EXEC
- EXEC Privilege

Command History	**Version 8.3.16.1** Introduced the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show clock
12:30:04.402 pacific Tue May 22 2012
Dell#
```

Example (Detail)

```
Dell#show clock detail
12:30:26.892 pacific Tue May 22 2012
Time source is RTC hardware
Summer time starts 00:00:00 UTC Wed Mar 14 2012
Summer time ends 00:00:00 pacific Wed Nov 7 2012
Dell#
```

Related Commands

clock summer-time recurring — displays the time and date from the switch hardware clock.

show calendar — displays the time and date from the switch hardware clock.

show ntp associations

Display the NTP master and peers.

Syntax `show ntp associations`

Command Modes

- EXEC
- EXEC Privilege

Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show ntp associations` command shown in the following example.

Field	Description
(none)	One or more of the following symbols could be displayed: • * means synchronized to this peer. • # means almost synchronized to this peer. • + means the peer was selected for possible synchronization. • - means the peer is a candidate for selection. • ~ means the peer is statically configured.
remote	Displays the remote IP address of the NTP peer.
ref clock	Displays the IP address of the remote peer's reference clock.

Field	Description
st	Displays the peer's stratum, that is, the number of hops away from the external time source. A 16 in this column means the NTP peer cannot reach the time source.
when	Displays the last time the switch received an NTP packet.
poll	Displays the polling interval (in seconds).
reach	Displays the reachability to the peer (in octal bitstream).
delay	Displays the time interval or delay for a packet to complete a round-trip to the NTP time source (in milliseconds).
offset	Displays the relative time of the NTP peer's clock to the switch clock (in milliseconds).
disp	Displays the dispersion.

Example

```
Dell#show ntp associations
remote        ref clock  st when poll reach delay  offset disp
=============================================================
 10.10.120.5  0.0.0.0       16   -   256    0 0.00 0.000
16000.0
*172.16.1.33  127.127.1.0   11   6   16     377   -0.08
-1499.9 104.16
 172.31.1.33  0.0.0.0       16   -   256    0 0.00 0.000
16000.0
 192.200.0.2  0.0.0.0       16   -   256    0 0.00 0.000
16000.0
* master (synced), # master (unsynced), + selected, - candidate
Dell#
```

Related Commands

show ntp status — displays the current NTP status.

show ntp status

Display the current NTP status.

Syntax `show ntp status`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show ntp status` command shown in the following example.

Field	Description
“Clock is...”	States whether the switch clock is synchronized, which NTP stratum the system is assigned and the IP address of the NTP peer.
“frequency is...”	Displays the frequency (in ppm), stability (in ppm) and precision (in Hertz) of the clock in this system.
“reference time is...”	Displays the reference time stamp.
“clock offset is...”	Displays the system offset to the synchronized peer and the time delay on the path to the NTP root clock.
“root dispersion is...”	Displays the root and path dispersion.
“peer mode is...”	State what NTP mode the switch is. This should be Client mode.

Example

```
Dell#show ntp status
Clock is unsynchronized, stratum 16, no reference clock
frequency is 0.000 ppm, stability is 0.000 ppm, precision is
4294967279
reference time is 00000000.00000000 (6:28:16.000 UTC Thu Feb 7
2036)
clock offset is 0.000000 msec, root delay is 0.00000 sec
root dispersion is 0.00000 sec, peer dispersion is 0.000 msec
peer mode is unspec
Dell#
```

Related Commands

show ntp associations — displays information on the NTP master and peer configurations.

55

Tunneling

Tunneling is supported on the MXL platform.

tunnel-mode

Enable a tunnel interface.

Syntax	`tunnel mode {ipip	ipv6	ipv6ip}[decapsulate-any]` To disable an active tunnel interface, use the **no tunnel** `mode` command.
Parameters	

ipip	Enable tunnel in RFC 2003 mode and encapsulate IPv4 and/or IPv6 datagrams inside an IPv4 tunnel.
ipv6	Enable tunnel in RFC 2473 mode and encapsulate IPv4 and/or IPv6 datagrams inside an IPv6 tunnel.
ipv6ip	Enable tunnel in RFC 4213 mode and encapsulate IPv6 datagrams inside an IPv4 tunnel.
decapsulate-any	(Optional) Enable tunnel in multipoint receive-only mode.

Defaults	None
Command Modes	INTERFACE TUNNEL
Command History	

Version 9.4(0.0)	Added the decapsulate-any command.
Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To enable a tunnel interface, use this command. You must define a tunnel mode for the tunnel to function. If you previously defined the tunnel destination or source address, the tunnel mode must be compatible.

Including the decapsulate-any option causes the command to fail if any of the following tunnel transmit options are configured: tunnel destination, tunnel dscp, tunnel flow-label, tunnel hop-limit, or tunnel keepalive. Conversely, if you configure any tunnel allow-remote entries, the `tunnel—mode` command fails unless the decapsulate-any option is included

Configuration of IPv6 commands over decapsulate-any tunnel causes an error.

tunnel source

Set a source address for the tunnel.

Syntax

`tunnel source {ip-address | ipv6-address | interface-type-number}`

To delete the current tunnel source address, use the `no tunnel source` command.

Parameters

ip-address	Enter the source IPv4 address in A.B.C.D format.
ipv6–address	Enter the source IPv6 address in X:X:X:X::X format.
interface-type-number	• For a 100/1000 Ethernet interface, enter the keyword `GigabitEthernet` then the slot/port information. • For a 1–Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the slot/port information. • For a Port Channel interface, enter the keywords `port-channel` then a number from 1 to 128. • For a 10–Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

Defaults

none

Command Modes

INTERFACE TUNNEL (conf-if-tu)

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

If you configure a tunnel interface or destination address, the tunnel source must be compatible.

If you configure a tunnel source address as an interface, the tunnel does not function until the compatible address is present on the particular interface.

tunnel keepalive

Configure the tunnel keepalive target, interval and attempts.

Syntax

```
tunnel keepalive {ip-address | ipv6-address}[interval
{seconds}] [attempts {count | unlimited}]
```

Use the **no tunnel keepalive** command to disable tunnel keepalive probes.

Parameters

ip-address ipv6 address	Enter the **IPv4 or IPv6 address** of the peer to which the keepalive probes will be sent.
interval seconds	Enter the keyword **interval** followed by the interval time, in seconds, after which the restart process to keepalive probe packets. The range is from 5- 255. Default range is 5.
count	(OPTIONAL) Enter the keyword **count** to count packets processed by the filter. The range is from 3-10, Default range is 3.
unlimited	Enter the keyword **unlimited** to specify the unlimited number of keepalive probe packets.

Defaults

Tunnel keepalive is disabled.

Command Modes

INTERFACE TUNNEL

Command History

Version 9.4(0.0)	Introduced on the MXL.

Usage Information

When configured, the system will send ICMP echo probe packets at the configured interval and expect a response within the configured number of attempts, else the tunnel interface will be declared operational down.

tunnel allow-remote

Configure an IPv4 or IPv6 address or prefix whose tunneled packets will be accepted for decapsulation. If no allow-remote entries are configured, tunneled packets from any remote peer address will be accepted.

Syntax

tunnel allow-remote `{ip-address | ipv6-address} [mask]`

Use the **no tunnel allow-remote** command to delete a configured allow-remote entry. Any specified address/mask values must match an existing entry for the delete to succeed. If the address and mask are not specified, this command deletes all allow-remote entries.

Parameters

ip-address	Enter the source IPv4 address in A.B.C.D format.
ipv6–address	Enter the source IPv6 address in X:X:X:X::X format.
mask	(OPTIONAL) Enter a network mask in /prefix format (/x) or A.B.C.D to match a range of remote addresses. The default mask is /32 for IPv4 addresses and /128 for IPv6 addresses, which match only the specified address.

Defaults

If no tunnel allow remote is configured, all traffic which is destined to tunnel source address will be decapsulated.

Command Modes

INTERFACE TUNNEL

Command History

Version 9.4(0.0)	Introduced on the MXL.

Usage Information

Up to eight allow-remote entries can be configured on any particular multipoint receive-only tunnel.

This command will fail if the address family entered does not match the outer header address family of the tunnel mode, tunnel source, or any other tunnel allow-remote.

If any allow-remote are configured, the tunnel source or tunnel mode commands will fail if the outer header address family does not match that of the configured allow-remote.

tunnel dscp

Configure the method to set the DSCP in the outer tunnel header.

Syntax

```
tunnel dscp {mapped | <value>}
```

To use the default tunnel mapping behavior, use the `no tunnel dscp value` command.

Parameters

mapped	Enter the keyword `mapped` to map the original packet DSCP (IPv4)/Traffic Class (IPv6) to the tunnel header DSCP (IPv4)/ Traffic Class (IPv6) depending on the mode of tunnel.
value	Enter a value to set the DSCP value in the tunnel header. The range is from 0 to 63. The default value of **0** denotes mapping of original packet DSCP (IPv4)/Traffic Class (IPv6) to the tunnel header DSCP (IPv4)/Traffic Class (IPv6) depending on the mode of tunnel.

Defaults	0 (Mapped)
Command Modes	INTERFACE TUNNEL (conf-if-tu)
Command History	Version 9.3(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	This command configures the method used to set the high 6 bits (the differentiated services codepoint) of the IPv4 TOS or the IPv6 traffic class in the outer IP header. A value of 0 copies original packet DSCP (IPv4)/Traffic Class (IPv6) to the tunnel header DSCP (IPv4)/Traffic Class (IPv6) depending on the mode of tunnel.

tunnel destination

Set a destination endpoint for the tunnel.

Syntax `tunnel destination {ip-address | ipv6-address}`

To delete a tunnel destination address, use the `no tunnel destination {ip-address | ipv6-address}` command.

Parameters

ip-address	Enter the destination IPv4 address for the tunnel.
ipv6–address	Enter the destination IPv6 address for the tunnel.

Defaults	none
Command Modes	INTERFACE TUNNEL (conf-if-tu)
Command History	Version 9.3(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	The tunnel interface is inoperable without a valid tunnel destination address for the configured Tunnel mode. To establish a logical tunnel to the particular destination address, use the destination address of the outer tunnel header. If you configure a tunnel interface or source address, the tunnel destination must be compatible.

tunnel flow-label

Configure the method to set the IPv6 flow label value in the outer tunnel header.

Syntax	`tunnel flow-label value` To return to the default value of 0, use the `no tunnel flow-label value` command.
Parameters	*value* — Enter a value to set the IPv6 flow label value in the tunnel header. The range is from 0 to 1048575. The default value is **0**.
Defaults	**0** (Mapped original packet flow-label value to tunnel header flow-label value)
Command Modes	INTERFACE TUNNEL (conf-if-tu)
Command History	Version 9.3(0.0) — Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	This command is only valid for tunnel interfaces with an IPv6 outer header.

tunnel hop-limit

Configure the method to set the IPv4 time-to-live or the IPv6 hop limit value in the outer tunnel header.

Syntax	`tunnel hop-limit value` To restore the default tunnel hop-limit, use the `no tunnel hop-limit` command.
Parameters	*value* — Enter the hop limit (ipv6) or time-to-live (ipv4) value to include in the tunnel header. The range is from 0 to 255. The default is **64**.
Defaults	**64** (Time-to-live for IPv4 outer tunnel header or hop limit for IPv6 outer tunnel header)
Command Modes	INTERFACE TUNNEL (conf-if-tu)
Command History	Version 9.3(0.0) — Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information	A value of 0 copies the inner packet hop limit (ipv6) or time-to-live (ipv4) in the encapsulated packet to the tunnel header hop limit (ipv6) or time-to-live (ipv4) value.

ip unnumbered

Configure a tunnel interface to operate without a unique explicit IPv4 address and select the interface from which the tunnel will borrow its address.

Syntax

ip unnumbered `{interface-type interface-number}`

Use the **no ip unnumbered** command to set the tunnel back to default logical address. If the tunnel was previously operational, this will make the tunnel interface operationally down, unless the tunnel also has an IPv6 address configured..

Parameters

interface-type interface-number	Enter the interface type, followed by a slot number.

Defaults

None

Command Modes

INTERFACE TUNNEL

Command History

Version 9.4(0.0)	Introduced on the MXL.

Usage Information

The ip unnumbered command will fail in two condition:

- If the logical ip address is configured.
- If the tunnel mode is ipv6ip (where ip address over tunnel interface is not possible).

To ping the unnumbered tunnels the logical address route information should be present in both the ends.

NOTE: The ip unnumbered command can specify an interface name that does not yet exist, or does not yet have a configured IPv6 address. The tunnel interface is not changed to the operationally up state until logically ip address is identified from the one of the address family.

ipv6 unnumbered

Configure a tunnel interface to operate without a unique explicit IPv6 address and select the interface from which the tunnel will borrow its address.

Syntax

ipv6 unnumbered *`{interface-type interface-number}`*

Use the **no ipv6 unnumbered** command to set the tunnel back to default logical address. If the tunnel was previously operational, this will make the tunnel interface operationally down, unless the tunnel also has an IPv4 address configured.

Parameters

interface-type interface-number	Enter the interface type, followed by the type, slot and port information.

Defaults

None.

Command Modes

INTERFACE TUNNEL

Command History

Version 9.4(0.0)	Introduced on the MXL.

Usage Information

The ip unnumbered command will fail in two condition:

- If the logical ip address is configured.
- If the tunnel mode is ipv6ip (where ip address over tunnel interface is not possible).

To ping the unnumbered tunnels the logical address route information should be present in both the ends.

NOTE: The ipv6 unnumbered command can specify an interface name that does not yet exist, or does not yet have a configured IPv6 address. But the tunnel interface will not go operationally up until it has determined a logical address to use of at least one address family.

56

u-Boot

All commands in this chapter are in u-Boot mode. These commands are supported on the Dell Networking Operating System (OS) MXL 10/40GbE Switch Module platform.

To access this mode, press any key when the following line appears on the console during a system boot.

```
Hit any key to stop autoboot:
```

Enter u-Boot immediately, as the `BOOT_USER#` prompt.

NOTE: This chapter describes only a few commands available in u-Boot mode.

NOTE: You cannot use the Tab key to complete commands in this mode.

boot change

Change the operating system boot parameters.

Syntax	`boot change [primary	secondary	default]`
Command Modes	uBoot
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

boot selection

Change the ROM bootstrap bootflash partition.

Syntax	`boot selection [a	b]`
Command Modes	uBoot
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

boot show net config retries

Show the number of retries for network boot configuration failure.

Syntax	`boot show net config retries`
Command Modes	uBoot
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
BOOT_USER# boot show net config retries

Number of Network Boot Config Retries is : 0

BOOT_USER #
```

boot write net config retries

Set the number of retries for network boot configuration failure.

Syntax	`boot write net config retries <int>`
Command Modes	uBoot
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
BOOT_USER # boot write net config retries 2

Updated number of Network Boot Config retries to 2.

BOOT_USER #
```

boot zero

Clears the primary, secondary, or default boot parameters.

Syntax	`boot zero [primary	secondary	default]`
Command Modes	uBoot
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

default gateway

Set the default gateway IP address.

Syntax	`default-gateway <ip-address>`
Command Modes	uBoot
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

enable

Change the access privilege level.

Syntax	`enable [user	admin]`
Command Modes	uBoot
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

help

Display the help menu.

Syntax	`help`
Command Modes	uBoot
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
BOOT_USER # help
***** Dell Force10 Boot Interface Help Information *****
Current access level: USER LEVEL
Use "syntax help" for more information on syntax.
Available command list (22 commands total):
  boot change [primary|secondary|default]
    change operating system boot parameters
  boot selection [a|b]
    change the rom bootstrap bootflash partition
  boot show net config retries
    show number of retries for network boot config failure
  boot write net config retries <int>
    write number of retries for network boot config failure
  boot zero [primary|secondary|default]
    zero operating system boot parameters
  default-gateway <ip-address>
```

```
    default-gateway - set the default gateway ip address
  enable [user|admin]
     change access privilege level
  help
    display help menu
-(36%)-Use <CR> to continue, q to stop:
BOOT_USER #
```

ignore enable password

Ignore the enabled password.

Syntax	`ignore enable-password`	
Command Modes	uBoot	
Command History	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

ignore startup config

Ignore the system startup configuration.

Syntax	`ignore startup-config`	
Command Modes	uBoot	
Command History	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

interface management ethernet ip address

Set the management port IP address and mask.

Syntax	`interface management ethernet ip address <ip/mask>`	
Command Modes	uBoot	
Command History	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

no default-gateway

Clear the default gateway IP address.

Syntax	`no default-gateway`
Command Modes	uBoot
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

no interface management ethernet ip address

Clear the management port IP address and mask.

Syntax	`no interface management ethernet ip address`
Command Modes	uBoot
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

reload

Reload the MXL switch.

Syntax	`reload`
Command Modes	uBoot
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

show boot blc

Show the boot loop counter value.

Syntax	`show boot blc`
Command Modes	uBoot

Command History	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
BOOT_USER # show boot blc ?
Total 1 possible command found.
Possible command list:
  show boot blc
    show the boot loop counter value
BOOT_USER # show boot blc
Boot Loop Counter : 10

BOOT_USER #
```

show boot selection

Display the ROM bootstrap bootflash partition.

Syntax `show boot selection`

Command Modes uBoot

Command History	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
BOOT_USER # show boot selection

ROM BOOTSTRAP SELECTOR PARMETERS:
================================
Next ROM bootstrap set to occur from Bootflash partition A.

Last ROM bootstrap occurred from Bootflash partition B.

BOOT_USER #
```

show bootflash

Show summary of boot flash information.

Syntax `show bootflash`

Command Modes uBoot

Command History	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
BOOT_USER # show bootflash

GENERAL BOOTFLASH INFO
======================
Bootflash Partition A:
  Dell Force10 Networks System Boot
  Official IOM_LP_IMG_BOOT_LOADER, BSP Release 4.0.1.0bt1
  Created Tue May 1 10:56:16 2012 by build on login-sjc-01

Bootflash Partition B:
  Dell Force10 Networks System Boot
  Official IOM_LP_IMG_BOOT_LOADER, BSP Release 4.0.1.0bt1
  Created Tue May 1 10:56:16 2012 by build on login-sjc-01

Boot Selector Partition:
  Dell Force10 Networks System Boot
  Official IOM_XLOAD_LP_IMG_BOOT_SELECTOR, BSP Release
4.0.0.0bt1
  Created Tue May 1 10:56:34 2012 by build on login-sjc-01

BOOT_USER #
```

show bootvar

Show summary of operating system boot parameters.

Syntax

```
show bootvar
```

Command Modes

uBoot

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
BOOT_USER # show bootvar

PRIMARY OPERATING SYSTEM BOOT PARAMETERS:
========================================
boot device                        : tftp
file name                          : premnath
Management Etherenet IP address    : 10.16.130.134/16
Server IP address                  : 10.16.127.35
Default Gateway IP address         : 15.0.0.1
Management Etherenet MAC address : 00:01:E8:43:DE:DF

SECONDARY OPERATING SYSTEM BOOT PARAMETERS:
========================================
No Operating System boot parameters specified!

DEFAULT OPERATING SYSTEM BOOT PARAMETERS:
========================================
boot device                        : tftp
file name                          : FTOS-XL-8-3-16-99.bin
Management Etherenet IP address    : 10.16.130.134/16
Server IP address                  : 10.16.127.53
Default Gateway IP address         : 15.0.0.1
Management Etherenet MAC address : 00:01:E8:43:DE:DF

BOOT_USER #
```

show default-gateway

Display the default gateway IP address.

Syntax	`show default-gateway`	
Command Modes	uBoot	
Command History	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
BOOT_USER # show default-gateway

Gateway IP address: 15.0.0.1

BOOT_USER #
```

show interface management Ethernet

Show the management port IP address and mask.

Syntax	`show interface management ethernet`	
Command Modes	uBoot	
Command History	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
BOOT_USER # show interface management ethernet

Management ethernet IP address: 10.16.130.134/16

BOOT_USER #
```

show interface management port config

Show the management port boot characteristics.

Syntax	`show interface management port config`	
Command Modes	uBoot	
Command History	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
BOOT_USER # show interface management port config

Management ethernet Port Configuration: no Auto Negotiate
Management ethernet Port Configuration: 100M

Management ethernet Port Configuration: full duplex

BOOT_USER #
```

syntax help

Show the syntax information.

Syntax	`help`
Command Modes	uBoot
Command History	Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
BOOT_USER # help
***** Dell Force10 Boot Interface Help Information *****
Current access level: USER LEVEL
Use "syntax help" for more information on syntax.
Available command list (22 commands total):
  boot change [primary|secondary|default]
    change operating system boot parameters
  boot selection [a|b]
    change the rom bootstrap bootflash partition
  boot show net config retries
    show number of retries for network boot config failure
  boot write net config retries <int>
    write number of retries for network boot config failure
  boot zero [primary|secondary|default]
    zero operating system boot parameters
  default-gateway <ip-address>
    default-gateway - set the default gateway ip address
  enable [user|admin]
    change access privilege level
  help
    display help menu
-(36%)-Use <CR> to continue, q to stop:
BOOT_USER #
```

57

Uplink Failure Detection (UFD)

Uplink failure detection (UFD) provides detection of the loss of upstream connectivity and, if you use this with network interface controller (NIC) teaming, automatic recovery from a failed link.

clear ufd-disable

Re-enable one or more downstream interfaces on the switch/router that are in a UFD-Disabled Error state so that an interface can send and receive traffic.

Syntax `clear ufd-disable {interface interface | uplink-state-group group-id}`

Parameters

interface *interface*	Specify one or more downstream interfaces. For *interface*, enter one of the following interface types: • Fast Ethernet: `fastethernet {slot/port | slot/port-range}` • 10 Gigabit Ethernet: `tengigabitethernet {slot/port |slot/ port-range}` • 40 Gigabit Ethernet: `fortygigabitethernet {slot/port |slot/ port-range}` • Port channel: `port-channel {1-512 | port-channel-range}` Where `port-range` and `port-channel-range` specify a range of ports separated by a dash (-) and/or individual ports/port channels in any order; for example: `gigabitethernet 1/1-2,5,9,11-12 port-channel 1-3,5`. A comma is required to separate each port and port-range entry.
uplink-state-group *group-id*	Re-enables all UFD-disabled downstream interfaces in the group. The valid group-id values are from 1 to 16.

Command Modes EXEC Mode

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

- downstream — assigns a port or port-channel to the uplink-state group as a downstream interface.

- upstream — assigns a port or port-channel to the uplink-state group as an upstream interface.
- uplink-state-group — creates an uplink-state group and enables the tracking of upstream links.

debug uplink-state-group

Enable debug messages for events related to a specified uplink-state group or all groups.

Syntax	`debug uplink-state-group [group-id]` To turn off debugging event messages, enter the `no debug uplink-state-group [group-id]` command.
Parameters	***group-id*** — Enables debugging on the specified uplink-state group. The valid group-id values are from 1 to 16.
Defaults	none
Command Modes	EXEC Privilege
Command History	**Version 8.3.16.1** — Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	clear ufd-disable — re-enables downstream interfaces that are in a UFD-Disabled Error state.

description

Enter a text description of an uplink-state group.

Syntax	`description text`
Parameters	***text*** — Text description of the uplink-state group. The maximum length is 80 alphanumeric characters.
Defaults	none
Command Modes	UPLINK-STATE-GROUP
Command History	**Version 8.3.16.1** — Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell(conf-uplink-state-group-3)#description Testing UFD feature
Dell(conf-uplink-state-group-3)#show config
!
```

```
uplink-state-group 3
  description Testing UFD feature
```

Related Commands

[uplink-state-group](#) — creates an uplink-state group and enables the tracking of upstream links.

downstream

Assign a port or port-channel to the uplink-state group as a downstream interface.

Syntax

`downstream interface`

To delete an uplink-state group, enter the `no downstream interface` command.

Parameters

interface	Enter one of the following interface types: • 10 Gigabit Ethernet: `tengigabitethernet {slot/port	slot/port-range}` • 40 Gigabit Ethernet: `fortygigabitethernet {slot/port |slot/port-range}` • Port channel: `port-channel {1-512	port-channel-range}` Where `port-range` and `port-channel-range` specify a range of ports separated by a dash (-) and/or individual ports/port channels in any order; for example: `gigabitethernet 1/1-2,5,9,11-12 port-channel 1-3,5`. A comma is required to separate each port and port-range entry.

Defaults

none

Command Modes

UPLINK-STATE-GROUP

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

You can assign physical port or port-channel interfaces to an uplink-state group.

You can assign an interface to only one uplink-state group. Configure each interface assigned to an uplink-state group as either an upstream or downstream interface, but not both.

You can assign individual member ports of a port channel to the group. An uplink-state group can contain either the member ports of a port channel or the port channel itself, but not both.

Related Commands	- downstream — assigns a port or port-channel to the uplink-state group as a downstream interface. - upstream — assigns a port or port-channel to the uplink-state group as an upstream interface. - uplink-state-group — creates an uplink-state group and enables the tracking of upstream links.

downstream auto-recover

Enable auto-recovery so that UFD-disabled downstream ports in an uplink-state group automatically come up when a disabled upstream port in the group comes back up.

Syntax	`downstream auto-recover` To disable auto-recovery on downstream links, use the `no downstream auto-recover` command.
Defaults	The auto-recovery of UFD-disabled downstream ports is enabled.
Command Modes	UPLINK-STATE-GROUP
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands	- downstream — assigns a port or port-channel to the uplink-state group as a downstream interface. - upstream — assigns a port or port-channel to the uplink-state group as an upstream interface. - uplink-state-group — creates an uplink-state group and enables the tracking of upstream links.

downstream disable links

Configure the number of downstream links in the uplink-state group that are disabled if one upstream link in an uplink-state group goes down.

Syntax	`downstream disable links {`*`number`*` |all}` To revert to the default setting, use the `no downstream disable links` command.
Parameters	*number* — Enter the number of downstream links to be brought down by UFD. The range is from 1 to 1024.

all	Brings down all downstream links in the group.

Defaults

All

Command Modes

UPLINK-STATE-GROUP

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

A user-configurable number of downstream interfaces in an uplink-state group are put into a link-down state with an UFD-Disabled error message when one upstream interface in an uplink-state group goes down.

If all upstream interfaces in an uplink-state group go down, all downstream interfaces in the same uplink-state group are put into a link-down state.

Related Commands

- downstream — assigns a port or port-channel to the uplink-state group as a downstream interface.
- upstream — assigns a port or port-channel to the uplink-state group as an upstream interface.
- uplink-state-group — creates an uplink-state group and enables the tracking of upstream links.

enable

Re-enable upstream-link tracking for an uplink-state group after it has been disabled.

Syntax

`enable`

To disable upstream-link tracking without deleting the uplink-state group, use the `no enable` command.

Parameters

group-id	Enables debugging on the specified uplink-state group. The valid group-id values are from 1 to 16.

Defaults

Upstream-link tracking is automatically enabled in an uplink-state group.

Command Modes

UPLINK-STATE-GROUP

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

- uplink-state-group — creates an uplink-state group and enables the tracking of upstream links.

show running-config uplink-state-group

Display the current configuration of one or more uplink-state groups.

Syntax `show running-config uplink-state-group [group-id]`

Parameters

group-id	Displays the current configuration of all uplink-state groups or a specified group. The valid group-id values are from 1 to 16.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show running-config uplink-state-group
!
uplink-state-group 3
  no enable
  description Testing UFD feature
  downstream disable links 2
  downstream TenGigabitEthernet 0/1-2,5,9,11-12
  upstream TenGigabitEthernet 0/3-4
```

Related Commands

- show uplink-state-group — displays the status information on a specified uplink-state group or all groups.
- uplink-state-group — creates an uplink-state group and enables the tracking of upstream links.

show uplink-state-group

Display status information on a specified uplink-state group or all groups.

Syntax `show uplink-state-group [group-id] [detail]`

Parameters

group-id	Displays status information on a specified uplink-state group or all groups. The valid group-id values are from 1 to 16.
detail	Displays additional status information on the upstream and downstream interfaces in each group

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History		
	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell# show uplink-state-group
Uplink State Group: 1 Status: Enabled, Up
Uplink State Group: 3 Status: Enabled, Up
Uplink State Group: 5 Status: Enabled, Down
Uplink State Group: 6 Status: Enabled, Up
Uplink State Group: 7 Status: Enabled, Up
Uplink State Group: 16 Status: Disabled, Up

Dell# show uplink-state-group 16
Uplink State Group: 16 Status: Disabled, Up

Dell#show uplink-state-group detail
(Up): Interface up (Dwn): Interface down (Dis): Interface
disabled
Uplink State Group      : 1 Status: Enabled, Up
Upstream Interfaces     :
Downstream Interfaces   :

Uplink State Group      : 3 Status: Enabled, Up
Upstream Interfaces     : Gi 0/46(Up) Gi 0/47(Up)
Downstream Interfaces   : Te 13/0(Up) Te 13/1(Up) Te 13/3(Up)
Te 13/5(Up) Te 13/6(Up)

Uplink State Group      : 5 Status: Enabled, Down
Upstream Interfaces     : Gi 0/0(Dwn) Gi 0/3(Dwn) Gi 0/5(Dwn)
Downstream Interfaces   : Te 13/2(Dis) Te 13/4(Dis) Te
13/11(Dis) Te 13/12(Dis) Te 13/13(Dis) Te 13/14(Dis) Te
13/15(Dis)

Uplink State Group      : 6 Status: Enabled, Up
Upstream Interfaces     :
Downstream Interfaces   :

Uplink State Group      : 7 Status: Enabled, Up
Upstream Interfaces     :
Downstream Interfaces   :

Uplink State Group      : 16 Status: Disabled, Up
Upstream Interfaces     : Gi 0/41(Dwn) Po 8(Dwn)
Downstream Interfaces   : Gi 0/40(Dwn)
```

Related Commands

- show running-config uplink-state-group — displays the current configuration of one or more uplink-state groups.
- uplink-state-group — create an uplink-state group and enables the tracking of upstream links.

uplink-state-group

Create an uplink-state group and enable the tracking of upstream links on a switch/ router.

Syntax `uplink-state-group` *`group-id`*

To delete an uplink-state group, enter the `no uplink-state-group group-id` command.

To disable upstream-link tracking without deleting the uplink-state group, use the `no enable` command in Uplink-State-Group Configuration mode.

Parameters

group-id	Enter the ID number of an uplink-state group. The range is from 1 to 16.

Defaults none

Command Modes CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module..

Usage Information

After you enter the command, to assign upstream and downstream interfaces to the group, enter Uplink-State-Group Configuration mode.

An uplink-state group is considered to be operationally up if at least one upstream interface in the group is in the Link-Up state.

An uplink-state group is considered to be operationally down if no upstream interfaces in the group are in the Link-Up state. No uplink-state tracking is performed when a group is disabled or in an operationally down state.

Example

```
Dell(conf)#uplink-state-group 16
Dell(conf)#
02:23:17: %STKUNIT0-M:CP %IFMGR-5-ASTATE_UP: Changed uplink
state group Admin
state to up: Group 16
```

Related Commands

- show running-config uplink-state-group — displays the current configuration of one or more uplink-state groups.
- show uplink-state-group — displays the status information on a specified uplink-state group or all groups.

upstream

Assign a port or port-channel to the uplink-state group as an upstream interface.

Syntax `upstream interface`

To delete an uplink-state group, use the `no upstream interface` command.

Parameters

interface	Enter one of the following interface types:

- 10 Gigabit Ethernet: `tengigabitethernet {`*`slot/port | slot/port-range`*`}`
- 40 Gigabit Ethernet: `fortygigabitethernet {`*`slot/port | slot/port-range`*`}`
- Port channel: `port-channel {`*`1-512 | port-channel-range`*`}`

Where `port-range` and `port-channel-range` specify a range of ports separated by a dash (-) and/or individual ports/port channels in any order; for example: `gigabitethernet 1/1-2,5,9,11-12 port-channel 1-3,5`. A comma is required to separate each port and port-range entry.

Defaults	none
Command Modes	UPLINK-STATE-GROUP
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

You can assign physical port or port-channel interfaces to an uplink-state group.

You can assign an interface to only one uplink-state group. Configure each interface assigned to an uplink-state group as either an upstream or downstream interface, but not both.

You can assign individual member ports of a port channel to the group. An uplink-state group can contain either the member ports of a port channel or the port channel itself, but not both.

Example

```
Dell(conf-uplink-state-group-16)# upstream gigabitethernet
1/10-15
Dell(conf-uplink-state-group-16)#
```

Related Commands

- downstream — assigns a port or port-channel to the uplink-state group as a downstream interface.
- upstream — assigns a port or port-channel to the uplink-state group as an upstream interface.
- uplink-state-group — creates an uplink-state group and enables the tracking of upstream links.

58

VLAN Stacking

With the virtual local area network (VLAN)-stacking feature (also called stackable VLANs and QinQ), you can "stack" VLANs into one tunnel and switch them through the network transparently.

For more information about basic VLAN commands, refer to the *Virtual LAN (VLAN) Commands* section in the Layer 2 chapter.

Important Points to Remember

- If you do not enable the spanning tree protocol (STP) across the stackable VLAN network, STP bridge protocol data units (BPDUs) from the customer's networks are tunneled across the stackable VLAN network.
- If you do enable STP across the stackable VLAN network, STP BPDUs from the customer's networks are consumed and not tunneled across the stackable VLAN network unless you enable protocol tunneling.
- Layer 3 protocols are not supported on a stackable VLAN network.
- Assigning an IP address to a stackable VLAN is supported when all the members are only stackable VLAN trunk ports. IP addresses on a stackable VLAN-enabled VLAN are not supported if the VLAN contains stackable VLAN access ports. This facility is provided for the simple network management protocol (SNMP) management over a stackable VLAN-enabled VLAN containing only stackable VLAN trunk interfaces. Layer 3 routing protocols on such a VLAN are not supported.
- Dell Networking OS recommends that you do not use the same MAC address, on different customer VLANs, on the same stackable VLAN.
- Interfaces configured using stackable VLAN access or stackable VLAN trunk commands do not switch traffic for the default VLAN. These interfaces are switch traffic only when they are added to a non-default VLAN.

dei enable

Make packets eligible for dropping based on their drop eligible indicator (DEI) value.

Syntax	`dei enable`
Defaults	Packets are colored green; no packets are dropped.
Command Modes	CONFIGURATION
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

dei honor

Honor the incoming DEI value by mapping it to a system drop precedence. Enter the command once for 0 and once for 1.

Syntax

```
dei honor {0 | 1} {green | red | yellow}
```

Parameters

0 | 1	Enter the bit value you want to map to a color.
green | red | yellow	Choose a color: • `Green`: High priority packets that are the least preferred to be dropped. • `Yellow`: Lower priority packets that are treated as best-effort. • `Red`: Lowest priority packets that are always dropped (regardless of congestion status).

Defaults

Disabled; Packets with an unmapped DEI value are colored green.

Command Modes

INTERFACE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

You must first enable DEI for this configuration to take effect.

Related Commands

dei enable — enables DEI.

dei mark

Set the DEI value on egress according to the color currently assigned to the packet.

Syntax

```
dei mark {green | yellow} {0 | 1}
```

Parameters

0 | 1	Enter the bit value you want to map to a color.
green | yellow	Choose a color: • `Green`: High priority packets that are the least preferred to be dropped. • `Yellow`: Lower priority packets that are treated as best-effort.

Defaults

All the packets on egress are marked with DEI 0.

Command Modes	INTERFACE
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	You must first enable DEI for this configuration to take effect.
Related Commands	dei enable — enables DEI.

member

Assign a stackable VLAN access or trunk port to a VLAN. The VLAN must contain the `vlan-stack compatible` command in its configuration.

Syntax

`member interface`

To remove an interface from a Stackable VLAN, use the `no member interface` command.

Parameters

interface	Enter the following keywords and slot/port or number information: • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabyte Ethernet interface, enter the keyword `fortyGigE` then the slot/ port information.

Defaults	Not configured.
Command Modes	conf-if-vl-<vlan-id>-stack
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	You must enable the stackable VLAN (using the `vlan-stack compatible` command) on the VLAN prior to adding a member to the VLAN.
Related Commands	vlan-stack compatible — enables stackable VLAN on a VLAN.

show interface dei-honor

Display the dei honor configuration.

Syntax `show interface dei-honor [interface slot/port]`

Parameters

interface slot/ port	Enter the interface type then the line card slot and port number.

Command Modes EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show interface dei-honor

Default Drop precedence: Green
Interface   CFI/DEI          Drop precedence
---------------------------------------------
Gi 0/1      0                Green
Gi 0/1      1                Yellow
Gi 8/9      1                Red
Gi 8/40     0                Yellow
```

Related Commands dei honor — honors the incoming DEI value.

show interface dei-mark

Display the dei mark configuration.

Syntax `show interface dei-mark [interface slot/port]`

Parameters

interface slot/ port	Enter the interface type then the line card slot and port number.

Command Modes EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show interface dei-mark

Default CFI/DEI Marking: 0
Interface   Drop precedence      CFI/DEI
------------------------------------------------
Gi 0/1      Green                0
Gi 0/1      Yellow               1
Gi 8/9      Yellow               0
Gi 8/40     Yellow               0
```

Related Commands	dei mark — sets the DEI value on egress.

vlan-stack access

Specify a Layer 2 port or port channel as an access port to the stackable VLAN network.

Syntax	`vlan-stack access` To remove access port designation, use the `no vlan-stack access` command.
Defaults	Not configured.
Command Modes	INTERFACE
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	Prior to enabling this command, to place the interface in Layer 2 mode, enter the `switchport` command. To remove the access port designation, remove the port (using the `no member interface` command) from all stackable VLAN enabled VLANs.

vlan-stack compatible

Enable the stackable VLAN feature on a VLAN.

Syntax	`vlan-stack compatible` To disable the Stackable VLAN feature on a VLAN, use the `no vlan-stack compatible` command.
Defaults	Not configured.
Command Modes	CONF-IF-VLAN
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	Prior to disabling the stackable VLAN feature, remove the members. To view the stackable VLANs, use the `show vlan` command in EXEC Privilege mode. Stackable VLANs contain members, designated by the M in the Q column of the command output.

Example

```
Dell#show vlan

Codes: * - Default VLAN, G - GVRP VLANs

   NUM  Status    Q Ports
*  1    Inactive
   2    Active    M Gi 13/13
                  M Gi 13/0-2
   3    Active    M Po1(Gi 13/14-15)
                  M Gi 13/18
                  M Gi 13/3
   4    Active    M Po1(Gi 13/14-15)
                  M Gi 13/18
                  M Gi 13/4
   5    Active    M Po1(Gi 13/14-15)
                  M Gi 13/18
                  M Gi 13/5
Dell#
```

vlan-stack dot1p-mapping

Map C-Tag dot1p values to a S-Tag dot1p value. You can separate the C-Tag values by commas and dashed ranges are permitted. Dynamic mode CoS overrides any Layer 2 QoS configuration in case of conflicts.

Syntax `vlan-stack dot1p-mapping c-tag-dot1p` *`values`* `sp-tag-dot1p` *`value`*

Parameters

c-tag-dot1p *value*	Enter the keyword `c-tag-dot1p` then the customer dot1p value that is mapped to a service provider do1p value. The range is from 0 to 5.
sp-tag-dot1p *value*	Enter the keyword `sp-tag-dot1p` then the service provider dot1p value. The range is from 0 to 5.

Defaults none

Command Modes INTERFACE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

vlan-stack protocol-type

Define the stackable VLAN tag protocol identifier (TPID) for the outer VLAN tag (also called the VMAN tag). If you do not configure this command, the system assigns the value 0x9100.

Syntax `vlan-stack protocol-type` *`number`*

Parameters	*number*	Enter the hexadecimal number as the stackable VLAN tag. You may specify both bytes of the 2-byte S-Tag TPID. The range is from 0 to FFFF. The default is **9100**.

Defaults

0x9100

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

For specific interoperability limitations regarding the S-Tag TPID, refer to the *Dell Networking OS Configuration Guide*.

Related Commands

portmode hybrid — sets a port (physical ports only) to accept both tagged and untagged frames. A port configured this way is identified as a hybrid port in report displays.

vlan-stack trunk — specifies a Layer 2 port or port channel as a trunk port to the Stackable VLAN network.

vlan-stack trunk

Specify a Layer 2 port or port channel as a trunk port to the Stackable VLAN network.

Syntax

`vlan-stack trunk`

To remove a trunk port designation from the selected interface, use the `no vlan-stack trunk` command.

Defaults

Not configured.

Command Modes

INTERFACE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Prior to using this command, to place the interface in Layer 2 mode, execute the `switchport` command.

To remove the trunk port designation, first remove the port (using the `no member interface` command) from all stackable VLAN-enabled VLANs.

Starting with the Dell Networking OS version 7.8.1.0, a VLAN-Stack trunk port is also allowed to be configured as a tagged port and as an untagged port for single-tagged VLANs. When the VLAN-Stack trunk port is also a member of an untagged VLAN, the port must be in Hybrid mode. Refer to portmode hybrid.

In the first example, a VLAN-Stack trunk port is configured and then also made part of a single-tagged VLAN.

In the second example, the tag protocol identifier (TPID) is set to 8848. The "Gi 3/10" port is configured to act as a VLAN-Stack access port, while the "TenGi 8/0" port acts as a VLAN-Stack trunk port, switching stackable VLAN traffic for VLAN 10, while also switching untagged traffic for VLAN 30 and tagged traffic for VLAN 40. (To allow VLAN 30 traffic, the native VLAN feature is required, by executing the `portmode hybrid` command. Refer to portmode hybrid in the Interfaces chapter.

Example

```
Dell(conf-if-gi-0/42)#switchport
Dell(conf-if-gi-0/42)#vlan-stack trunk
Dell(conf-if-gi-0/42)#show config
!
interface GigabitEthernet 0/42
  no ip address
  switchport
  vlan-stack trunk
  no shutdown
Dell(conf-if-gi-0/42)#interface vlan 100
Dell(conf-if-vl-100)#vlan-stack compatible
Dell(conf-if-vl-100-stack)#member gigabitethernet 0/42
Dell(conf-if-vl-100-stack)#show config
!
interface Vlan 100
  no ip address
  vlan-stack compatible
  member GigabitEthernet 0/42
  shutdown
Dell(conf-if-vl-100-stack)#interface vlan 20
Dell(conf-if-vl-20)#tagged gigabitethernet 0/42
Dell(conf-if-vl-20)#show config
!
interface Vlan 20
  no ip address
  tagged GigabitEthernet 0/42
  shutdown
Dell(conf-if-vl-20)#do show vlan
Codes: * - Default VLAN, G - GVRP VLANs
Q: U - Untagged, T - Tagged
   x - Dot1x untagged, X - Dot1x tagged
   G - GVRP tagged, M - Vlan-stack

  NUM  Status Description   Q Ports
* 1    Inactive
  20   Active               T Gi 0/42
  100  Active               M Gi 0/42
Dell(conf-if-vl-20)#
```

Example

```
Dell(config)#vlan-stack protocol-type 88A8
Dell(config)#interface gigabitethernet 3/10
Dell(conf-if-gi-3/10)#no shutdown
Dell(conf-if-gi-3/10)#switchport
Dell(conf-if-gi-3/10)#vlan-stack access
Dell(conf-if-gi-3/10)#exit
Dell(config)#interface tenGigabitethernet 8/0
Dell(conf-if-te-10/0)#no shutdown
Dell(conf-if-te-10/0)#portmode hybrid
Dell(conf-if-te-10/0)#switchport
Dell(conf-if-te-10/0)#vlan-stack trunk
Dell(conf-if-te-10/0)#exit

Dell(config)#interface vlan 20
Dell(conf-if-vlan)#vlan-stack compatible
Dell(conf-if-vlan)#member Gi 7/0, Gi 3/10, TenGi 8/0
Dell(conf-if-vlan)#exit

Dell(config)#interface vlan 20
Dell(conf-if-vlan)#untagged TenGi 8/0
Dell(conf-if-vlan)#exit
Dell(config)#

Dell(config)#interface vlan 40
Dell(conf-if-vlan)#tagged TenGi 8/0
Dell(conf-if-vlan)#exit
Dell(config)#
```

59

Virtual Link Trunking (VLT)

VLT allows physical links between two chassis to appear as a single virtual link to the network core.

VLT eliminates the requirement for Spanning Tree protocols by allowing link aggregation group (LAG) terminations on two separate distribution or core switches, and by supporting a loop-free topology. VLT provides Layer 2 multipathing, creating redundancy through increased bandwidth and enabling multiple parallel paths between nodes and load-balancing traffic where alternative paths exist.

Prerequisites: Before you configure VLT, ensure both VLT peer switches are running the same Dell Networking Operating System (OS) version and are configured for rapid spanning tree protocol (RSTP) as described in the *Virtual Link Trunking (VLT)* chapter in the *Dell Networking OS Configuration Guide*.

back-up destination

Configure the IP address of the management interface on the remote VLT peer to be used as the endpoint of the VLT backup link for sending out-of-band hello messages.

Syntax

```
back-up destination ip-address [interval seconds]}
```

Parameters

ip–address	Enter the IPv4 or IPv6 address of the backup destination.
interval *seconds*	Enter the keyword `interval` to specify the time interval to send hello messages. The range is from 1 to 5 seconds. The default is 1 second.

Defaults	Not configured.
Command Modes	VLT DOMAIN
Usage Information	You can only enable either IPv4 or IPv6.

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

clear ip mroute

Clear learned multicast routes on the multicast forwarding table. To clear the protocol-independent multicast (PIM) tree information base, use the `clear ip pim tib` command.

Syntax

```
clear ip mroute {group-address [source-address] | * | snooping}
```

Parameters

group-address [*source-address*]	Enter the multicast group address and source address (if desired), in dotted decimal format, to clear information on a specific group.
*	Enter `*` to clear all multicast routes.
snooping	Enter the keyword `snooping` to delete multicast snooping route table entries.

Command Modes EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

clear ip pim tib

Clear PIM tree information from the PIM database.

Syntax

```
clear ip pim tib [group]
```

Parameters

group	(OPTIONAL) Enter the multicast group address in dotted decimal format (A.B.C.D).

Command Modes EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

If you use this command on a local VLT node, all multicast routes from the local PIM TIB, the entire multicast route table, and all the entries in the data plane are deleted. The entries in Peer PIM TIB (Sync) are not deleted but are marked for re-download. Both local and synced routes are removed from the multicast route table. The peer VLT node clears synced routes from the node.

If you use this command on a peer VLT node, only the synced routes are deleted from the multicast route table.

lacp ungroup member-independent vlt

Prevent possible loop during the bootup of a VLT peer switch or a device that accesses the VLT domain.

Syntax

```
lacp ungroup member-independent vlt
```

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

LACP on the VLT ports (on a VLT switch or access device), which are members of the virtual link trunk, is not brought up until the VLT domain is recognized on the access device.

multicast peer-routing timeout

Configure the time for a VLT node to retain synced multicast routes or synced multicast outgoing interface (OIF) after a VLT peer node failure.

Syntax

```
multicast peer-routing timeout value
```

To restore the default value, use the `no multicast peer-routing timeout` command.

Parameters

value	Enter the timeout value in seconds. The range is from 1 to 1200. The default is 150.

Default

Not configured.

Command Modes

VLT DOMAIN (conf-vlt-domain)

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

peer-link port-channel

Configure the specified port channel as the chassis interconnect trunk between VLT peers in the domain.

Syntax

```
peer-link port-channel id-number
```

Parameters

id-number	Enter the port-channel number that acts as the interconnect trunk. The range is from 1 to 128.

Defaults	Not configured.
Command Modes	VLT DOMAIN
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.

peer-routing

Enable L3 VLT peer-routing. This command is applicable for both IPV6/ IPV4.

Syntax

```
peer-routing
```

To disable L3 VLT peer-routing, use the `no peer-routing` command.

Defaults Disabled.

Command Modes VLT DOMAIN (conf-vlt-domain)

Command History

Version 9.4(0.0)	Added the IPV6/IPV4 support on the MXL.
Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

peer-routing-timeout

Configure the timeout for the software to wait before connecting to a VLT peer with a Down status. This command is applicable for both IPV6/ IPV4.

Syntax

```
peer-routing-timeout value
```

To restore the default value, use the `no peer-routing-timeout` command.

Parameters

value	Enter the timeout value in seconds. The range is from 1 to 65535. The default value is 0 (no timeout).

Command Modes VLT DOMAIN (conf-vlt-domain)

Command History

Version 9.4(0.0)	Added the IPV6/IPV4 support on the MXL.
Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information When the timer expires, the software checks to see if the VLT peer is now available. If the VLT peer is not available, peer-routing is disabled on that peer.

primary-priority

Reconfigure the primary role of VLT peer switches.

Syntax	`primary-priority` *`value`*
Parameters	*value* — To configure the primary role on a VLT peer, enter a lower value than the priority value of the remote peer. The range is from 1 to 65535.
Default	**32768**
Command Modes	VLT DOMAIN
Command History	Version 9.2(0.0) — Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	After you configure the VLT domain on each peer switch on both sides of the interconnect trunk, by default, the software elects a primary and secondary VLT peer device. To reconfigure the primary role of VLT peer switches, use the `priority` command.

show ip mroute

View the multicast routing table.

Syntax

```
show ip mroute [static | group-address [source-address] | count
| snooping [vlan vlan-id] [group-address [source-address]] |
summary | vlt [group-address | count]
```

Parameters

Static	(OPTIONAL) Enter the keyword `static` to view static multicast routes.
group-address [source-address]	(OPTIONAL) Enter the multicast group-address to view only routes associated with that group. Enter the source-address to view routes with that group-address and source-address.
count	(OPTIONAL) Enter the keyword `count` to view the number of multicast routes and packets.
snooping [vlan *vlan-id*] [*group-address* [*source-address*]]	(OPTIONAL) Enter the keyword `snooping` to display information on the multicast routes PIM-SM snooping discovers. Enter a VLAN ID to limit the information displayed to the multicast routes PIM-SM snooping discovers on a specified VLAN. The VLAN ID range is from 1 to 4094.

	Enter a multicast group address and, optionally, a source multicast address in dotted decimal format (A.B.C.D) to limit the information displayed to the multicast routes PIM-SM snooping discovers for a specified multicast group and source.
summary	(OPTIONAL) Enter the keyword `summary` to view routes in a tabular format.
vlt	(OPTIONAL) Enter the keyword `vlt` to view multicast routes with a spanned incoming interface. Enter a multicast group address in dotted decimal format (A.B.C.D) to limit the information displayed to the multicast routes for a specified multicast group.
count	Enter the keyword `count` to display VLT route and packet data.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show ip mroute` command shown in the examples.

Field	Description
(S, G)	Displays the forwarding entry in the multicast route table.
uptime	Displays the amount of time the entry has been in the multicast forwarding table.
Incoming interface	Displays the reverse path forwarding (RPF) information towards the source for (S,G) entries and the RP for (*,G) entries.
Outgoing interface list:	Lists the interfaces that meet one of the following: • a directly connected member of the Group • statically configured member of the Group • received a (*,G) or (S,G) Join message

Example (static)

```
Dell#show ip mroute static
Mroute: 23.23.23.0/24, interface: Lo 2
Protocol: static, distance: 0, route-map: none, last change:
00:00:23
```

Example (snooping)

```
Dell#show ip mroute snooping
IPv4 Multicast Snooping Table (*, 224.0.0.0), uptime 17:46:23
Incoming vlan: Vlan 2
Outgoing interface list:
GigabitEthernet 4/13
```

```
(*, 225.1.2.1), uptime 00:04:16
Incoming vlan: Vlan 2
Outgoing interface list:
GigabitEthernet 4/11
GigabitEthernet 4/13

(165.87.1.7, 225.1.2.1), uptime 00:03:17
Incoming vlan: Vlan 2
Outgoing interface list:
GigabitEthernet 4/11
GigabitEthernet 4/13
GigabitEthernet 4/20
GigabitEthernet 4/13
GigabitEthernet 4/20
```

Example (detail)

```
Dell#show ip mroute
IP Multicast Routing Table

(*, 224.10.10.1), uptime 00:05:12
Incoming interface: GigabitEthernet 3/12
Outgoing interface list:
GigabitEthernet 3/13

(1.13.1.100, 224.10.10.1), uptime 00:04:03
Incoming interface: GigabitEthernet 3/4
Outgoing interface list:
GigabitEthernet 3/12
GigabitEthernet 3/13

(*, 224.20.20.1), uptime 00:05:12
Incoming interface: GigabitEthernet 3/12
Outgoing interface list:
GigabitEthernet 3/4
utgoing interface l
GigabitEthernet 3/4
```

show vlt backup-link

Displays information on the backup link operation.

Syntax `show vlt backup-link`

Default Not configured.

Command Modes EXEC

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell# show vlt backup-link

VLT Backup Link
-----------------
Destination:                 10.11.198.130
Peer HeartBeat status:       Up
HeartBeat Timer Interval:    1
HeartBeat Timeout:           3
```

```
UDP Port:                    34998
HeartBeat Messages Sent:     634
HeartBeat Messages Received: 473
```

show vlt brief

Displays summarized status information about VLT domains currently configured on the switch.

Syntax	`show vlt brief`
Default	Not configured.
Command Modes	EXEC
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.

Example (Brief)

```
Dell# show vlt brief
VLT Domain Brief
------------------
Domain ID:                        1000
Role:                             Primary
Role Priority:                    700
ICL Link Status:                  Up
HeartBeat Status:                 Up
VLT Peer Status:                  Up
Local Unit Id:                    0
Version:                          6(1)
Local System MAC address:         00:01:e8:d7:3f:bd
Remote System MAC address:        00:01:e8:d7:3f:cf
Configured System MAC address:    00:00:00:0a:0a:0a
Remote system version:            6(1)
Delay-Restore timer:              90 seconds
Peer-Routing :                    Disabled
Peer-Routing-timeout timer:       0 seconds
Multicast peer-routing timeout: 150 seconds
Dell#
```

show vlt detail

Displays detailed status information about VLT domains currently configured on the switch.

Syntax	`show vlt detail`
Default	Not configured.
Command Modes	EXEC
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell# show vlt detail
Local LAG Id Peer LAG Id Local Status Peer Status Active VLANs
------------ ----------- ------------ ----------- -------------
128          128         UP           UP          1000
Dell#
```

show vlt inconsistency

Display deviations in VLT multicast traffic.

Syntax `show vlt inconsistency ip mroute`

Command Modes EXEC

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show vlt inconsistency ip mroute
Spanned Multicast Routing IIF Inconsistency

Multicast Route                  LocalIIF      PeerIIF
---------------                  ----------    ---------
(22.22.22.200, 225.1.1.2)         VLAN 5       VLAN 6
(*, 225.1.1.2)                    VLAN 15      te 0/5
Dell#
```

show vlt mismatch

Configure the time for a VLT node to retain synced multicast routes or synced multicast OIF after VLT peer node failure.

Syntax `show vlt mismatch`

Command Modes EXEC

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show vlt mismatch
Domain
-----------
Parameters   Local             Peer
------------ -----------        ---------
System-Mac   00:00:00:0a:0a:0a 00:00:00:00:00:00

Vlan-config
------------
Vlan-ID Local Mode     Peer Mode
--------- ------------ -----------
2000    --             L2
```

```
3000    L3              --
Dell#
```

show vlt role

Displays the VLT peer status, role of the local VLT switch, VLT system MAC address and system priority, and the MAC address and priority of the local VLT device.

Syntax `show vlt role`

Default Not configured.

Command Modes EXEC

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show vlt role
VLT Role
----------
VLT Role:                    Primary
System MAC address:          00:00:00:0a:0a:0a
Primary Role Priority:       700
Local System MAC address:    00:01:e8:d7:3f:bd
Local System Role Priority: 700
Local Unit Id:                0
Dell#
```

show vlt statistics

Displays statistics on VLT operations.

Syntax `show vlt statistics`

Default Not configured.

Command Modes EXEC

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show vlt statistics
VLT Domain Statistics
-----------------------
HeartBeat Messages Sent:     646
HeartBeat Messages Received: 484
ICL Hello's Sent:            162
ICL Hello's Received:        162
Domain Mismatch Errors:      0
Version Mismatch Errors:     0
Config Mismatch Errors:      14
```

```
VLT MAC Statistics
--------------------
L2 Info Pkts sent:65,   L2 Mac-sync Pkts Sent:88
L2 Info Pkts Rcvd:82,   L2 Mac-sync Pkts Rcvd:61
L2 Reg Request sent:17
L2 Reg Request rcvd:15

L2 Reg Response sent:12
L2 Reg Response rcvd:11

VLT Igmp-Snooping Not Enabled

VLT ARP Statistics
--------------------
ARP Tunnel Pkts sent:0
ARP Tunnel Pkts Rcvd:0
ARP Tunnel Pkts sent Non Vlt:0
ARP Tunnel Pkts Rcvd Non Vlt:0
ARP-sync Pkts Sent:0
ARP-sync Pkts Rcvd:0
ARP Reg Request sent:18
ARP Reg Request rcvd:16

VLT NDP Statistics
--------------------
NDP NA VLT Tunnel Pkts sent:0
NDP NA VLT Tunnel Pkts Rcvd:0
NDP NA Non-VLT Tunnel Pkts sent:0
NDP NA Non-VLT Tunnel Pkts Rcvd:0
Ndp-sync Pkts Sent:0
Ndp-sync Pkts Rcvd:0
Ndp Reg Request sent:17
Ndp Reg Request rcvd:15

VLT Multicast Statistics
-------------------------------
Info Pkts Sent: 0
Info Pkts Rcvd: 0
Reg Request Sent: 0
Reg Request Rcvd: 0
Reg Response Sent: 0
Reg Response Rcvd: 0
Route updates sent to Peer: 0
Route updates rcvd from Peer: 0
Route update pkts sent to Peer: 0
Route update pkts rcvd from Peer: 0
```

system-mac

Reconfigure the default MAC address for the domain.

Syntax `system-mac` *`mac-address`*

Parameters

mac-address	Enter the system MAC address for the VLT domain.

Defaults Automatically assigned based on the primary priority and MAC address of each VLT peer.

Command Modes	VLT DOMAIN
Command History	**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

When you create a VLT domain on a switch, the system automatically creates a VLT-system MAC address used for internal system operations.

To explicitly define the MAC address for the domain, use the `system-mac` command.

You must also reconfigure the same MAC address on the VLT peer switch.

Use this command to minimize the time required for the VLT system to synchronize the default MAC address of the VLT domain on both peer switches when one peer switch reboots.

unit-id

Explicitly configure the default unit ID of a VLT peer switch.

Syntax `unit-id id`

Parameters

id	Enter the system unit ID for VLT. The range is from 0 to 1.

Defaults Automatically assigned based on the MAC address of each VLT peer. The peer with the lower MAC address is assigned unit 0; the peer with the higher MAC address is assigned unit 1.

Command Modes VLT DOMAIN

Command History

Version 9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

When you create a VLT domain on a switch, the system automatically assigns a unique unit ID (0 or 1) to each peer switch. The unit IDs are used for internal system operations. To explicitly configure the unit ID of a VLT peer, use the `unit-id` command. Configure a different unit ID (0 or 1) on each peer switch.

To minimize the time required for the VLT system to determine the unit ID assigned to each peer switch when one peer reboots, use this command.

vlt domain

Enable VLT on a switch, configure a VLT domain, and enter VLT-domain configuration mode.

Syntax	`vlt domain domain-id`
Parameters	*domain-id* — Enter the Domain ID number. Configure the same domain ID on the peer switch. VLT uses the domain ID to automatically create a VLT MAC address for the domain. The range of domain IDs is from 1 to 1000.
Command Modes	CONFIGURATION
Command History	Version 9.2(0.0) — Introduced on the MXL 10/40GbE Switch IO Module.

vlt-peer-lag port-channel

Associate the port channel to the corresponding port channel in the VLT peer for the VLT connection to an attached device.

Syntax	`vlt-peer-lag port-channel id-number`
Parameters	*id-number* — Enter the port-channel number that connects to another port channel in the VLT peer. The range is from 1 to 128.
Defaults	Not configured.
Command Modes	INTERFACE PORT-CHANNEL
Command History	Version 9.2(0.0) — Introduced on the MXL 10/40GbE Switch IO Module.

show vlt private-vlan

Display the association of private VLAN (PVLAN) with the VLT LAG. You can configure VLT peer nodes in a PVLAN on the MXL switch.

Syntax	`show vlt private-vlan`
Command Modes	EXEC
Command History	Version 9.3(0.0) — Introduced on the MXL 10/40GbE Switch IO Module platform.

Usage Information

If you add an ICL or VLTi link as a member of a primary VLAN, the ICL becomes a part of the primary VLAN and its associated secondary VLANs, similar to the behavior for normal trunk ports. VLAN symmetricity is not validated if you associate an ICL to a PVLAN. Similarly, if you dissociate an ICL from a PVLAN, although the PVLAN symmetrictiy exists, ICL is removed from that PVLAN in such a case. The **ICL Status** field denotes the type of the VLAN port of the VLTi link configured in a PVLAN.

Example

```
Dell#Show vlt private-vlan vlan-id

Codes: C- Community, I - Isolated, V - Internally tagged, T -
tagged, * - VLT Pvlan
Primary    Secondary    ICL Status
10                        V (*)
            20(C)        V
            30 (I)      V

40                        T
            50(C)        T
            60 (I)      T


Dell#
```

60

Virtual Router Redundancy Protocol (VRRP)

Virtual router redundancy protocol (VRRP) is supported by the Dell Networking Operating System (OS) for IPv4 and IPv6.

The following commands apply to both VRRP IPv4 and IPv6:

- advertise-interval
- description
- disable
- hold-time
- preempt
- priority
- show config
- track
- virtual-address

VRRP Ipv6 are in the VRRP for IPv6 Commands section.

advertise-interval

Set the time interval between VRRP advertisements.

Syntax

```
advertise-interval {seconds | centisecs centisecs}
```

To return to the default settings, use the `no advertise-interval` command.

Parameters

seconds	Enter a number of seconds. The range is from 1 to 255. The default is **1 second**.
centisecs *centisecs*	Enter the keyword `centisecs` followed by the number of centisecs in multiple of 25 centisecs. The range is `25` to `4075` centisecs in multiples of `25` centisecs.

Defaults **1 second or 100 centisecs**

Command Modes INTERFACE-VRRP

Command History

Version 9.5(0.0)	Introduced the support for centisecs on the MXL 10/40GbE Switch .

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information Dell Networking OS recommends keeping the default setting for this command. If you do change the time interval between VRRP advertisements on one router, change it on all routers.

authentication-type

Enable authentication of VRRP data exchanges.

Syntax `authentication-type simple [`*`encryption-type`*`]` *`password`*

To delete an authentication type and password, use the `no authentication-type` command.

Parameters

simple	Enter the keyword `simple` to specify simple authentication.
encryption-type	(OPTIONAL) Enter one of the following numbers: • `0` (zero) specifies an un-encrypted authentication data follows. • `7` (seven) specifies a hidden authentication data follows.
password	Enter a character string up to eight characters long as a password. If you do not enter an encryption-type, the password is stored as clear text.

Defaults Not configured.

Command Modes VRRP

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information The given password is encrypted by the system and the `show config` displays an encrypted text string for any of the encrypted typed used.

clear counters vrrp

Clear the counters maintained on VRRP operations.

Syntax `clear counters vrrp [`*`vrrp-id`*`]`

Parameters

vrrp-id	(OPTIONAL) Enter the number of the VRRP group ID. The range is from 1 to 255.

Command Modes	EXEC Privilege
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

debug vrrp

Allows you to enable debugging of VRRP.

Syntax

```
debug vrrp interface [vrrp-id] {all | packets | state | timer}
```

To disable debugging, use the `no debug vrrp interface [vrrp-id] {all | packets | state | timer}` command.

Parameters

interface	Enter the following keywords and slot/port or number information • For Port Channel interface types, enter the keywords `port-channel` then the number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a VLAN interface, enter the keyword `vlan` then the VLAN ID. The VLAN ID range is from 1 to 4094.
vrrp-id	(OPTIONAL) Enter a number from 1 to 255 as the VRRP group ID.
all	Enter the keyword `all` to enable debugging of all VRRP groups.
packets	Enter the keyword `packets` to enable debugging of VRRP control packets.
state	Enter the keyword `state` to enable debugging of VRRP state changes.
timer	Enter the keyword `timer` to enable debugging of the VRRP timer.

Command Modes	EXEC Privilege
Command History	**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	If you do not specify options, debug is active on all interfaces and all VRRP groups.

description

Configure a short text string describing the VRRP group.

Syntax	`description text` To delete a VRRP group description, use the `no description` command.
Parameters	***text*** — Enter a text string up to 80 characters long.
Defaults	Not enabled.
Command Modes	VRRP
Command History	**Version 8.3.16.1** — Introduced on the MXL 10/40GbE Switch IO Module.

disable

Disable a VRRP group.

Syntax	`disable` To re-enable a disabled VRRP group, use the `no disable` command.
Defaults	Enabled.
Command Modes	VRRP
Command History	**Version 8.3.16.1** — Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	To enable VRRP traffic, assign an IP address to the VRRP group using the `virtual-address` command and enter `no disable`.
Related Commands	virtual-address — specifies the IP address of the virtual router.

hold-time

Specify a delay (in seconds) before a switch becomes the MASTER virtual router. By delaying the initialization of the VRRP MASTER, the new switch can stabilize its routing tables.

Syntax	`hold-time {seconds	centisecs centisecs}` To return to the default value, use the `no hold-time` command.

Parameters

seconds	Enter a number of seconds. The range is from 0 to 65535. The default is **zero (0) seconds**.
centisecs *centisecs*	Enter the keyword `centisecs` then the number of centisecs in units of `25` centisecs. The range is from `0` to `65525` in units of `25` centisecs.

Defaults **zero (0) seconds**

Command Modes VRRP

Command History

Version 9.5(0.0)	Introduced the support for centisecs on the MXL 10/40GbE Switch.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information If a switch is a MASTER and you change the hold timer, disable and re-enable VRRP for the new hold timer value to take effect.

Related Commands disable — disables a VRRP group.

preempt

To preempt or become the MASTER router, permit a BACKUP router with a higher priority value.

Syntax `preempt`

To prohibit preemption, use the `no preempt` command.

Defaults Enabled (that is, a BACKUP router can preempt the MASTER router).

Command Modes VRRP

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

priority

Specify a VRRP priority value for the VRRP group. The VRRP protocol uses this value during the MASTER election process.

Syntax `priority` *`priority`*

To return to the default value, use the `no priority` command.

Parameters	*priority*	Enter a number as the priority. Enter 255 only if the router's virtual address is the same as the interface's primary IP address (that is, the router is the OWNER). The range is from 1 to 255. The default is **100**.

Defaults	**100**
Command Modes	VRRP

Command History	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To guarantee that a VRRP group becomes MASTER, configure the VRRP group's virtual address with same IP address as the interface's primary IP address and change the priority of the VRRP group to 255.

If you set the `priority` command to 255 and the `virtual-address` is not equal to the interface's primary IP address, an error message appears.

NOTE: Configuring VRRP priority 255 on an interface on which DHCP Client is enabled is not supported.

show config

View the non-default VRRP configuration.

Syntax

```
show config [verbose]
```

Parameters	verbose	(OPTIONAL) Enter the keyword `verbose` to view all VRRP group configuration information, including defaults.

Command Modes	VRRP

Command History	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell(conf-if-vrid-4)#show con
 vrrp-group 4
  virtual-address 119.192.182.124
 !
```

show vrrp

View the VRRP groups that are active. If no VRRP groups are active, the system returns `No Active VRRP group`.

Syntax

```
show vrrp [vrrp-id] [interface] [brief]
```

Parameters

vrrp-id	(OPTIONAL) Enter the Virtual Router Identifier for the VRRP group to view only that group. The range is from 1 to 255.
interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For Port Channel interface types, enter the keywords `port-channel` then the number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a VLAN interface, enter the keyword `vlan` then the VLAN ID. The VLAN ID range is from 1 to 4094.
brief	(OPTIONAL) Enter the keyword `brief` to view a table of information on the VRRP groups.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show vrrp brief` command shown in the following example.

Item	Description
Interface	Lists the interface type, slot and port on which the VRRP group is configured.
Grp	Displays the VRRP group ID.
Pri	Displays the priority value assigned to the interface. If the `track` command is configured to track that interface and the interface is disabled, the cost is subtracted from the priority value assigned to the interface.
Pre	States whether preempt is enabled on the interface. • `Y` = Preempt is enabled. • `N` = Preempt is not enabled.
State	Displays the operational state of the interface by using one of the following:

Item	Description
	• NA/IF (the interface is not available). • MASTER (the interface associated with the MASTER router). • BACKUP (the interface associated with the BACKUP router).
Master addr	Displays the IP address of the MASTER router.
Virtual addr(s)	Displays the virtual IP addresses of the VRRP routers associated with the interface.

Example (Brief)

```
Dell>Interface Grp Pri Pre State Master addr Virtual addr(s)
Description-----------------------------------------------------
-
TenGig 10/37 1 100 Y Master 200.200.200.200 200.200.200.201
TenGig10/37  2 100 Y Master 200.200.200.200 200.200.200.202
200.200.200.203
Description
TenGig10/37  3 100 Y Master 1.1.1.1 1.1.1.2
TenGig10/37  4 100 Y Master 200.200.200.200 200.200.200.206
200.200.200.207 ... short
desc

Dell>
```

Usage Information

The following describes the `show vrrp` command shown in the following example.

Item	Description
GigabitEthernet 12/3...	Displays the Interface, the VRRP group ID, and the network address. If the interface is not sending VRRP packets, 0.0.0.0 appears as the network address.
State: master...	Displays the interface's state: • Na/If (not available) • master (MASTER virtual router) • backup (BACKUP virtual router) the interface's priority and the IP address of the MASTER.
Hold Down:...	This line displays additional VRRP configuration information: • Hold Down displays the hold down timer interval in seconds. • Preempt displays TRUE if preempt is configured and FALSE if preempt is not configured. • AdvInt displays the Advertise Interval in seconds.
Adv rcvd:...	This line displays counters for the following:

Item	Description
	• Adv rcvd displays the number of VRRP advertisements received on the interface. • Adv sent displays the number of VRRP advertisements sent on the interface. • Gratuitous ARP sent displays the number of gratuitous ARPs sent.
Virtual MAC address	Displays the virtual MAC address of the VRRP group.
Virtual IP address	Displays the virtual IP address of the VRRP router to which the interface is connected.
Authentication:...	States whether authentication is configured for the VRRP group. If it is, the authentication type and the password are listed.
Tracking states..	This line is displayed if the `track` command is configured on an interface. Below this line, the following information on the tracked interface is displayed: • Dn or Up states whether the interface is down or up. • the interface type slot/port information.

Example

```
Dell>show vrrp
------------------
GigabitEthernet 12/3, VRID: 1, Net: 10.1.1.253
State: Master, Priority: 105, Master: 10.1.1.253 (local)
Hold Down: 0 sec, Preempt: TRUE, AdvInt: 1 sec
Adv rcvd: 0, Adv sent: 1862, Gratuitous ARP sent: 0
Virtual MAC address:
  00:00:5e:00:01:01
Virtual IP address:
  10.1.1.252
Authentication: (none)
Tracking states for 1 interfaces:
  Up GigabitEthernet 12/17 priority-cost 10
------------------
GigabitEthernet 12/4, VRID: 2, Net: 10.1.2.253
State: Master, Priority: 110, Master: 10.1.2.253 (local)
Hold Down: 10 sec, Preempt: TRUE, AdvInt: 1 sec
Adv rcvd: 0, Adv sent: 1862, Gratuitous ARP sent: 0
Virtual MAC address:
  00:00:5e:00:01:02
Virtual IP address:
  10.1.2.252
Authentication: (none)
Tracking states for 2 interfaces:
  Up GigabitEthernet 2/1 priority-cost 10
  Up GigabitEthernet 12/17 priority-cost 10
Dell>
```

track

Monitor an interface and lower the priority value of the VRRP group on that interface if it is disabled.

Syntax

`track interface [priority-cost cost]`

To disable monitoring, use the `no track interface` command.

Parameters

interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383. • For Port Channel interface types, enter the keywords `port-channel` then the number. The range is 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a VLAN interface, enter the keyword `vlan` then the VLAN ID. The VLAN ID range is from 1 to 4094.
cost	(OPTIONAL) Enter a number as the amount to be subtracted from the priority value. The range is 1 to 254. The default is **10**.

Defaults

cost = **10**

Command Modes

VRRP

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

If the interface is disabled, the cost value is subtracted from the priority value and forces a new MASTER election if the priority value is lower than the priority value in the BACKUP virtual routers.

virtual-address

Configure up to 12 IP addresses of virtual routers in the VRRP group. To start sending VRRP packets, set at least one virtual address for the VRRP group.

Syntax

`virtual-address ip-address1 [... ip-address12]`

To delete one or more virtual IP addresses, use the `no virtual-address ip-address1 [... ip-address12]` command.

Parameters

ip-address1	Enter an IP address of the virtual router in dotted decimal format. The IP address must be on the same subnet as the interface's primary IP address.

... ip-address12	(OPTIONAL) Enter up to 11 additional IP addresses of virtual routers in dotted decimal format. Separate the IP addresses with a space. The IP addresses must be on the same subnet as the interface's primary IP address.

Defaults Not configured.

Command Modes VRRP

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The VRRP group only becomes active and sends VRRP packets when a virtual IP address is configured. When you delete the virtual address, the VRRP group stops sending VRRP packets.

A system message appears after you enter or delete the `virtual-address` command.

To guarantee that a VRRP group becomes MASTER, configure the VRRP group's virtual address with the same IP address as the interface's primary IP address and change the priority of the VRRP group to 255.

You can ping the virtual addresses configured in all VRRP groups.

vrrp delay minimum

Set the delay time for VRRP initialization after an interface comes up.

Syntax `vrrp delay minimum` *`seconds`*

Parameters

seconds	Enter the number of seconds for the delay for VRRP initialization after an interface becomes operational. The range is from 0 to 900 (0 indicates no delay).

Defaults 0

Command Modes INTERFACE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

This command applies to a single interface. When used with the `vrrp delay reload` CLI, the later timer rules the VRRP enabling. For example, if `vrrp delay reload` is 600 and the `vrrp delay minimum` is 300:

- When the system reloads, VRRP waits 600 seconds (10 minutes) to bring up VRRP on all interfaces that are up and configured for VRRP.
- When an interface comes up, whether as part of a system reload or an interface reload, the system waits 300 seconds (5 minutes) to bring up VRRP on that interface.

Related Command	vrrp delay reload — sets the delay time for VRRP initialization after a system reboot.

vrrp delay reload

Set the delay time for VRRP initialization after a system reboot.

Syntax `vrrp delay reload seconds`

Parameters

seconds	Enter the number of seconds for the delay. The range is from 0 to 900 (0 indicates no delay).

Defaults 0

Command Modes INTERFACE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

This command applies to all the VRRP configured interfaces on a system. When used with the `vrrp delay minimum` CLI, the later timer rules the VRRP enabling. For example, if `vrrp delay reload` is 600 and the `vrrp delay minimum` is 300:

- When the system reloads, VRRP waits 600 seconds (10 minutes) to bring up VRRP on all interfaces that are up and configured for VRRP.
- When an interface comes up, whether as part of a system reload or an interface reload, the system waits 300 seconds (5 minutes) to bring up VRRP on that interface.

Save the configuration and reload the system for the delay timers to take effect.

Related Command	vrrp delay minimum — sets the delay time for VRRP initialization after a line card reboot.

vrrp-group

Assign a VRRP ID to an interface. You can configure up to 12 VRRP groups per interface.

Syntax `vrrp-group vrrp-id`

Parameters

vrrp-id	Enter a number as the group ID. The range is from 1 to 255.

Defaults Not configured.

Command Modes INTERFACE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information The VRRP group only becomes active and sends VRRP packets when a virtual IP address is configured. When you delete the virtual address, the VRRP group stops sending VRRP packets.

Related Command virtual-address — assigns up to 12 virtual IP addresses per VRRP group.

VRRP for IPv6 Commands

The following commands apply to IPv6.

clear counters vrrp ipv6

Clear the counters recorded for IPv6 VRRP groups.

Syntax `clear counters vrrp ipv6 [vrid | vrf instance]`

Parameters

vrid	(OPTIONAL) Enter the number of an IPv6 VRRP group. The range is from 1 to 255.
vrf *instance*	(OPTIONAL) Enter the name of a VRF instance (32 characters maximum) to clear the counters of all IPv6 VRRP groups in the specified VRF.

Defaults Not configured

Command Modes INTERFACE

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

debug vrrp ipv6

Allows you to enable debugging of VRRP.

Syntax

```
debug vrrp ipv6 interface [vrid] {all | packets | state |
timer}
```

Parameters

interface	Enter the following keywords and slot/port or number information: • For a Port Channel interface, enter the keywords `port-channel` then a number. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a VLAN interface, enter the keyword `vlan` then the VLAN ID. The VLAN ID range is from 1 to 4094.
vrid	(OPTIONAL) Enter a number from 1 to 255 as the VRRP group ID.
all	Enter the keyword `all` to enable debugging of all VRRP groups.
packets	Enter the keyword `packets` to enable debugging of VRRP control packets.
state	Enter the keyword `state` to enable debugging of VRRP state changes
timer	Enter the keyword `timer` to enable debugging of the VRRP timer.

Command Modes EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information If no options are specified, debug is active on all interfaces and all VRRP groups.

show vrrp ipv6

View the IPv6 VRRP groups that are active. If no VRRP groups are active, the system returns `No Active VRRP group`.

Syntax

```
show vrrp ipv6 [vrid] [interface] [brief]
```

Parameters

vrid	(OPTIONAL) Enter the virtual router identifier for the VRRP group to view only that group. The range is from 1 to 255.

interface	Enter the following keywords and slot/port or number information: • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For SONET interfaces, enter the keyword `sonet` then the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a VLAN interface, enter the keyword `vlan` then the VLAN ID. The VLAN ID range is from 1 to 4094.
brief	(OPTIONAL) Enter the keyword `brief` to view a table of information on the VRRP groups.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `show vrrp ipv6` command shown in the following example.

Line Beginning with	Description
GigabitEthernet...	Displays the Interface, the VRRP group ID, and the network address. If the interface is no sending VRRP packets, 0.0.0.0 appears as the network address.
VRF	VRF instance to which the interface (on which the VRRP group is configured) belongs.
State: master...	Displays the interface's state: • Na/If (not available). • master (MASTER virtual router). • backup (BACKUP virtual router). the interface's priority and the IP address of the MASTER.
Hold Down:...	This line displays additional VRRP configuration information: • Hold Down displays the hold down timer interval in seconds. • Preempt displays TRUE if preempt is configured and FALSE if preempt is not configured. • AdvInt displays the Advertise Interval in seconds.
Adv rcvd:...	This line displays counters for the following:

Line Beginning with	Description
	• Adv rcvd displays the number of VRRP advertisements received on the interface. • Adv sent displays the number of VRRP advertisements sent on the interface. • Bad pkts rcvd displays the number of invalid packets received on the interface.
Virtual MAC address	Displays the virtual MAC address of the VRRP group.
Virtual IP address	Displays the virtual IP address of the VRRP router to which the interface is connected.
Tracking states...	Displays information on the tracked interfaces or objects configured for a VRRP group (`track` command), including: • UP or DOWN state of the tracked interface or object (Up or Dn). • Interface type and slot/port or object number, description, and time since the last change in the state of the tracked object. • Cost to be subtracted from the VRRP group priority if the state of the tracked interface/object goes DOWN.

Example

```
Dell#show vrrp ipv6
------------------
GigabitEthernet 5/6, IPv6 VRID: 255, Version: 3, Net:
fe80::201:e8ff:fe7a:6bb9
VRF: 0 default-vrf
State: Master, Priority: 101, Master: fe80::201:e8ff:fe7a:6bb9
(local)
Hold Down: 0 centisec, Preempt: TRUE, AdvInt: 100 centisec
Accept Mode: FALSE, Master AdvInt: 100 centisec
Adv rcvd: 0, Bad pkts rcvd: 0, Adv sent: 64
Virtual MAC address:
  00:00:5e:00:02:ff
Virtual IP address:
  1::255 fe80::255
```

vrrp-ipv6-group

Assign an interface to a VRRP group.

Syntax `vrrp-ipv6-group` *`vrid`*

Parameters

vrid	Enter the virtual-router ID number of the VRRP group. The VRID range is from 1 to 255.

Defaults	Not configured.
Command Modes	INTERFACE
Command History	Version 8.3.16.1 — Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The VRRP group only becomes active and sends VRRP packets when a link-local virtual IP address is configured. When you delete the virtual address, the VRRP group stops sending VRRP packets.

- When VRF microcode is not loaded in CAM, the VRID for a VRRP group is the same as the VRID number configured with the `vrrp-group` or `vrrp-ipv6-group` command.
- When VRF microcode is loaded in CAM, the VRID for a VRRP group is equal to 16 times the `vrrp-group` or `vrrp-ipv6-group vrid` number plus the `ip vrf vrf-id` number. For example, if VRF microcode is loaded and VRRP group 10 is configured in VRF 2, the VRID used for the VRRP group is (16 x 10) + 2, or 162. This VRID value is used in the lowest byte of the virtual MAC address of the VRRP group and is also used for VRF routing.

NOTE: Configure the same VRID on neighboring routers (Dell Networking OS or non-Dell Networking OS) in the same VRRP group in order for all routers to interoperate.

version

Set VRRP protocol version for IPv4 group.

Syntax

```
version {2 | 3 | both}
```

To return to the default setting, use the `no version` command.

Parameters

2	Enter the `2` parameter to specify VRRP version 2 as defined by RFC 3768, *Virtual Router Redundancy Protocol.*
3	Enter the `2` parameter to specify VRRP version 3 as defined in RFC 5798, *Virtual Router Redundancy*.
both	Enter the `both` keyword for in-service migration from VRRP version 2 to VRRP version 3.

Defaults	2
Command Modes	VRRP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version 9.5(0.0)	Introduced on the Z9000, S6000, S4820T, S4810, and MXL.

Usage Information

You can use the version `both` command to migrate from VRRPv2 to VRRPv3. When you set the VRRP protocol version to both, the switch sends only VRRPv3 advertisements but can receive either VRRPv2 or VRRPv3 packets. To migrate an IPv4 VRRP group from VRRPv2 to VRRPv3:

1. Set the switches with the lowest priority to “both”.
2. Set the switch with the highest priority to version to 3.
3. Set all the switches from both to version 3.

> **NOTE:** Do not run VRRP version 2 and version 3 in the same group for an extended period of time.

Example

```
Dell(conf-if-te-0/0-vrid-100)#version ?
2                        VRRPv2
3                        VRRPv3
both                     Interoperable, send VRRPv3 receive
both

Dell(conf-if-te-0/0-vrid-100)#version 3
```

61

ICMP Message Types

This chapter lists and describes the possible ICMP message type resulting from a ping. The first three columns list the possible symbol or type/code. For example, you would receive a ! or 03 as an echo reply from your ping.

Table 1. ICMP Messages and Their Definitions

Symbol	Type	Code	Description	Query	Error
.			Timeout (no reply)		
!	0	3	echo reply	.	
U	3		destination unreachable:		
		0	network unreachable		.
		1	host unreachable		.
		2	protocol unreachable		.
		3	port unreachable		.
		4	fragmentation needed but don’t fragment bit set		.
		5	source route failed		.
		6	destination network unknown		.
		7	destination host unknown		.
		8	source host isolated (obsolete)		.
		9	destination network administratively prohibited		.
		10	destination host administratively prohibited		.
		11	network unreachable for TOS		.
		12	host unreachable for TOS		.
		13	communication administratively prohibited by filtering		.
		14	host precedence violation		.
		15	precedence cutoff in effect		.
C	4	0	source quench		.
	5		redirect		.

Symbol	Type	Code	Description	Query	Error
		0	redirect for network		.
		1	redirect for host		.
		2	redirect for type-of-service and network		.
		3	redirect for type-of-service and host		.
	8	0	echo request	.	
	9	0	router advertisement	.	
	10	0	router solicitation	.	
&	11		time exceeded:		
		0	time-to-live equals 0 during transit		.
		1	time-to-live equals 0 during reassembly		.
	12		parameter problem:		
		1	IP header bad (catchall error)		.
		2	required option missing		.
	13	0	timestamp request	.	
	14	0	timestamp reply	.	
	15	0	information request (obsolete)	.	
	16	0	information reply (obsolete)	.	
	17	0	address mask request	.	
	18	0	address mask reply	.	

62

SNMP Traps

This chapter lists the traps sent by the Dell Networking Operating System (OS). Each trap is listed by the fields Message ID, Trap Type, and Trap Option.

Table 2. SNMP Traps and Error Messages

Message ID	Trap Type	Trap Option
COLD_START	SNMP	COLDSTART
`%SNMP-5-SNMP_COLD_START: SNMP COLD_START trap sent.`		
WARM_START	SNMP	WARMSTART
COPY_CONFIG_COMPLETE	SNMP	NONE
`SNMP Copy Config Command Completed`		
LINK_DOWN	SNMP	LINKDOWN
`%IFA-1-PORT_LINKDN: changed interface state to down:%d`		
LINK_UP	SNMP	LINKUP
`%IFA-1-PORT_LINKUP: changed interface state to up: %d`		
AUTHENTICATION_FAIL	SNMP	AUTH
`%SNMP-3-SNMP_AUTH_FAIL: SNMP Authentication failed.Request with invalid community string.`		
EGP_NEIGHBOR_LOSS	SNMP	NONE
OSTATE_DOWN	SNMP	LINKDOWN
`%IFM-1-OSTATE_DN: changed interface state to down: %s`		
`%IFM-5-CSTATE_DN:Changed interface Physical state to down: %s`		
OSTATE_UP	SNMP	LINKUP
`%IFM-1-OSTATE_UP: changed interface state to up:%s`		
`%IFM-5-CSTATE_UP: Changed interface Physical state to up: %s`		
RMON_RISING_THRESHOLD	SNMP	NONE
`%RPM0-P:CP %SNMP-4-RMON_RISING_THRESHOLD: RMON rising threshold alarm from SNMP OID <oid>`		
RMON_FALLING_THRESHOLD	SNMP	NONE

Message ID	Trap Type	Trap Option
`%RPM0-P:CP %SNMP-4-RMON_FALLING_THRESHOLD: RMON falling threshold alarm from SNMP OID <oid>`		
RMON_HC_RISHING_THRESHOLD	SNMP	NONE
`%RPM0-P:CP %SNMP-4-RMON_HC_RISING_THRESHOLD: RMON high-capacity rising threshold alarm from SNMP OID <oid>`		
RMON_HC_FALLING_THRESHOLD	SNMP	NONE
`%RPM0-P:CP %SNMP-4-RMON_HC_FALLING_THRESHOLD: RMON high-capacity falling threshold alarm from SNMP OID <oid>`		
RESV	NONE	NONE
N/A		
CHM_MIN_ALRM_TEMP	ENVMON	TEMP
`%CHMGR-2-MINOR_TEMP: Minor alarm: chassis temperature`		
CHM_MIN_ALRM_TEMP_CLR	ENVMON	TEMP
`%CHMRG-5-MINOR_TEMP_CLR: Minor alarm cleared: chassis temperature normal (%s %d temperature is within threshold of %dC)`		
CHM_MAJ_ALRM_TEMP	ENVMON	TEMP
`%CHMGR-2-MAJOR_TEMP: Major alarm: chassis temperature high (%s temperature reaches or exceeds threshold of %dC)`		
CHM_MAJ_ALRM_TEMP_CLR	ENVMON	TEMP
`%CHMGR-2-MAJOR_TEMP_CLR: Major alarm cleared: chassis temperature lower (%s %d temperature is within threshold of %dC)`		
TME_TASK_SUSPEND	ENVMON	NONE
`%TME-2-TASK SUSPENDED: SUSPENDED - svce:%d - inst:%d - task:%s`		
TME_TASK_TERM	ENVMON	NONE
`%TME-2-ABNORMAL_TASK_TERMINATION: CRASH - task:%s %s`		
CHM_CPU_THRESHOLD	ENVMON	NONE
`%CHMGR-5-CPU_THRESHOLD: Cpu %s usage above threshold. Cpu5SecUsage (%d)`		
CHM_CPU_THRESHOLD_CLR	ENVMON	NONE
`%CHMGR-5-CPU_THRESHOLD_CLR: Cpu %s usage drops below threshold. Cpu5SecUsage (%d)`		
CHM_MEM_THRESHOLD	ENVMON	NONE

Message ID	Trap Type	Trap Option
`%CHMGR-5-MEM_THRESHOLD: Memory %s usage above threshold. MemUsage (%d)`		
CHM_MEM_THRESHOLD_CLR	ENVMON	NONE
`%CHMGR-5-MEM_THRESHOLD_CLR: Memory %s usage drops below threshold. MemUsage (%d)`		
MACMGR_STN_MOVE	ENVMON	NONE
`%MACMGR-5-DETECT_STN_MOVE: Station Move threshold exceeded for Mac %s in vlan %d`		
VRRP_BADAUTH	PROTO	NONE
`%RPM1-P:RP2 %VRRP-3-VRRP_BAD_AUTH: vrid-1 on Gi 11/12 rcvd pkt with authentication type mismatch.` `%RPM1-P:RP2 %VRRP-3-VRRP_BAD_AUTH: vrid-1 on Gi 11/12 rcvd pkt with authentication failure`		
VRRP_GO_MASTER	PROTO	NONE
`%VRRP-6-VRRP_MASTER: vrid-%d on %s entering MASTER`		
VRRP_PROTOCOL_ERROR	PROTO	NONE
`VRRP_PROTOERR: VRRP protocol error on %S`		
BGP4_ESTABLISHED	PROTO	NONE
`%TRAP-5-PEER_ESTABLISHED: Neighbor %a, state %s`		
BGP4_BACKW_XSITION	PROTO	NONE
`%TRAP-5-BACKWARD_STATE_TRANS: Neighbor %a, state %s`		
ETS_TRAP_TYPE_MODULE_STATUS_CHA NGE	ETS	NONE
`%DIFFSERV-5-ETS_TRAP_TYPE_MODULE_STATUS_CHANGE: ETS Module status changed to enabled` `%DIFFSERV-5-ETS_TRAP_TYPE_MODULE_STATUS_CHANGE: ETS Module status changed to disabled`		
ETS_TRAP_TYPE_ADMIN_MODE_CHANGE	ETS	NONE
`%DIFFSERV-5-ETS_TRAP_TYPE_ADMIN_MODE_CHANGE : ETS Admin mode changed to on for port %s` `%DIFFSERV-5-ETS_TRAP_TYPE_ADMIN_MODE_CHANGE : ETS Admin mode changed to off for port %s`		
ETS_TRAP_TYPE_OPER_STATE_CHANGE	ETS	NONE
`%DIFFSERV-5-ETS_TRAP_TYPE_OPER_STATE_CHANGE: ETS Oper state changed to init for port %s` `%DIFFSERV-5-ETS_TRAP_TYPE_OPER_STATE_CHANGE: ETS Oper state changed to off for port %s`		

Message ID	Trap Type	Trap Option
`%DIFFSERV-5-ETS_TRAP_TYPE_OPER_STATE_CHANGE: ETS Oper state changed to recommended for port %s`		
`%DIFFSERV-5-ETS_TRAP_TYPE_OPER_STATE_CHANGE: ETS Oper state changed to rxConfigSrc for port %s`		
ETS_TRAP_TYPE_PEER_STATE_CHANGE	ETS	NONE
`%DIFFSERV-5-ETS_TRAP_TYPE_PEER_STATE_CHANGE : ETS Peer state changed to enabled for port %s`		
`%DIFFSERV-5-ETS_TRAP_TYPE_PEER_STATE_CHANGE : ETS Peer state changed to disabled for port %s`		
PFC_TRAP_TYPE_MODULE_STATUS_CHANGE	PFC	NONE
`%DIFFSERV-5-PFC_TRAP_TYPE_MODULE_STATUS_CHANGE: PFC Module status changed to enabled`		
`%DIFFSERV-5-PFC_TRAP_TYPE_MODULE_STATUS_CHANGE: PFC Module status changed to disabled`		
PFC_TRAP_TYPE_ADMIN_MODE_CHANGE	PFC	NONE
`%DIFFSERV-5-PFC_TRAP_TYPE_ADMIN_MODE_CHANGE : PFC Admin mode changed to on for port %s`		
`%DIFFSERV-5-PFC_TRAP_TYPE_ADMIN_MODE_CHANGE : PFC Admin mode changed to off for port %s`		
PFC_TRAP_TYPE_OPER_STATE_CHANGE	PFC	NONE
`%DIFFSERV-5-PFC_TRAP_TYPE_OPER_STATE_CHANGE: PFC Oper state changed to init for port %s`		
`%DIFFSERV-5-PFC_TRAP_TYPE_OPER_STATE_CHANGE: PFC Oper state changed to off for port %s`		
`%DIFFSERV-5-PFC_TRAP_TYPE_OPER_STATE_CHANGE: PFC Oper state changed to recommended for port %s`		
`%DIFFSERV-5-PFC_TRAP_TYPE_OPER_STATE_CHANGE: PFC Oper state changed to rxConfigSrc for port %s`		
PFC_TRAP_TYPE_PEER_STATE_CHANGE	PFC	NONE
`%DIFFSERV-5-PFC_TRAP_TYPE_PEER_STATE_CHANGE: PFC Peer state changed to enabled for port %s`		
`%DIFFSERV-5-PFC_TRAP_TYPE_PEER_STATE_CHANGE: PFC Peer state changed to disabled for port %s`		
FIPS_MAX_FCF_LIMIT_RCH	FIPS	NONE
`%FCOE-5-MAX_FCF_LIMIT_RCH: Number of FCFs reached maximum allowed limit in VLAN %d`		
FIPS_MAX_ENODE_LIMIT_RCH	FIPS	NONE

Message ID	Trap Type	Trap Option
`%FCOE-5-MAX_ENODE_LIMIT_RCH: Number of ENodes reached maximum allowed limit in the system`		
FIPS_MAX_SESSION_LIMIT_RCH	FIPS	NONE
`%FCOE-5-MAX_SESSION_LIMIT_RCH: Number of sessions reached maximum allowed limit in the system`		
FIPS_FCF_DROP	FIPS	NONE
`%FCOE-5-FCF_DROP: New FCF(%d,%s) discovered in Vlan %d is dropped as max-FCF-limit per VLAN is reached`		
FIPS_ENODE_DROP	FIPS	NONE
`%FCOE-5-ENODE_DROP: New ENode(%d,%s) discovered in interface %s dropped as max-ENode-limit in system reached`		
FIPS_SESSION_DROP	FIPS	NONE
`%FCOE-5-SESSION_DROP: New session(%d,%s) request in interface %s dropped as max-session-limit in system reached`		
FIPS_ACL_INSTALL_FAIL	FIPS	NONE
`%FCOE-5-ACL_INSTALL_FAIL: problem in installing ACL entries due to no space or hardware failure`		
CHMGR_ENT_LAST_CHANGE_TIME	ENTITY	NONE
No error messages. Time, at which there is a change in a physical entity, is logged.		

63

FC Flex IO Modules

This part provides a generic, broad-level description of the operations, capabilities, and configuration commands of the Fiber Channel (FC) Flex IO module.

FC Flex IO Modules

This part provides a generic, broad-level description of the operations, capabilities, and configuration commands of the Fiber Channel (FC) Flex IO module.

Data Center Bridging (DCB) for FC Flex IO Modules

Data center bridging (DCB) refers to a set of IEEE Ethernet enhancements that provide data centers with a single, converged network to support multiple traffic types, including local area network (LAN), server, and storage traffic.

The Fibre Channel (FC) Flex IO module is supported on MXL 10/40GbE Switch. The MXL switch installed with the FC Flex IO module functions as a top-of-rack edge switch that supports converged enhanced ethernet (CEE) traffic — Fibre channel over Ethernet (FCoE) for storage, inter-process communication (IPC) for servers, and Ethernet local area network (LAN) (IP cloud) for data — as well as FC links to one or more storage area network (SAN) fabrics.

The `dcb-input` and `dcb-output` configuration commands are deprecated, starting with Dell Networking OS Release 9.3(0.0) on the MXL 10/40GbE Switch platform. Use the `dcp-map` command to create a DCB map to configure priority flow control (PFC) and enhanced transmission selection (ETS) on Ethernet ports that support converged Ethernet traffic.

The Dell Networking Operating System (OS) commands for the DCB features include 802.1Qbb priority-based flow control (PFC), 802.1Qaz enhanced transmission selection (ETS), and the data center bridging exchange (DCBX) protocol.

Interworking of DCB Map With DCB Buffer Threshold Settings

DCB map functionality is supported on the MXL platform.

The `dcb-input` and `dcb-output` configuration commands are deprecated. You must use the `dcp-map` command to create a DCB map to configure priority flow control (PFC) and enhanced transmission selection (ETS) on Ethernet ports that support converged Ethernet traffic.

Configure the `dcb-buffer-threshold` command and its related parameters only on ports with either auto configuration or dcb-map configuration. This command is not supported on existing front-panel interfaces or stack ports that are configured with the `dcb-input` or `dcb-output` commands. Similarly, if the dcb-buffer-threshold configuration is present on a stack port or any interface, the dcb-input or dcb-ouput policies cannot be applied on those interfaces.

Example: When the dcb-buffer-threshold policy is applied on interfaces or stack ports with the dcb-input or dcb-output policies, the following error message is displayed:

```
%Error: dcb-buffer-threshold not supported on interfaces with deprecated
commands
```

Example: When the dcb-input or dcb-output policy is configured on interfaces or stack ports with the dcb-buffer threshold policy, the following error message is displayed:

```
%Error: Deprecated command is not supported on interfaces with dcb-buffer-
threshold configured
```

You must not modify the service-class dot1p mappings when any buffer-threshold-policy is configured on the system.

```
S4810-1(conf)#service-class dot1p-mapping dot1p0 3

% Error: PFC buffer-threshold policies conflict with dot1p mappings. Please
remove all dcb-buffer-threshold policies to change mappings.
```

The `show dcb` command has been enhanced to display the following additional buffer-related information:

```
 S4810-YU-MR-Dell (conf)#do show dcb
 dcb Status :  Enabled
 PFC Queue Count :  2 --Indicate the PFC queue configured.
 Total buffer (lossy + lossless)(in KB): 7787--Total buffer space for lossy and
lossless queues
 PFC total buffer (in KB): 6526 --Indicates the total buffer (configured or
default)
 PFC shared buffer (in KB): 832--Indicates the shared buffer (Configured or
default)
 PFC available buffer ( in KB): 5694--Indicates remaining available buffers for
PFC that are free to be allocated
```

dcb-map

Create a DCB map to configure priority flow control (PFC) and enhanced transmission selection (ETS) on Ethernet ports that support converged Ethernet traffic. Apply the DCB map to an Ethernet interface.

Syntax	`dcb-map` *`map-name`*	
Parameters	*map-name*	Enter a DCB map name. The maximum number of alphanumeric characters is 32.
Defaults	None.	
Command Modes	CONFIGURATION INTERFACE	
Command History	Version 9.3(0.0)	Introduced on the FC Flex IO module installed in the MXL 10/40GbE Switch.

Usage Information	A DCB map is a template used to configure DCB parameters and apply them on converged Ethernet interfaces. DCB parameters include priority-based flow control (PFC) and enhanced traffic selection (ETS). To display the PFC and ETS settings in DCB maps, enter the `show qos dcb-map` command. Use the `dcb-map` command to create a DCB map to specify PFC and ETS settings and apply it on Ethernet ports. After you apply a DCB map to an interface, the PFC and ETS settings in the map are applied when the Ethernet port is enabled. DCBx is enabled on Ethernet ports by default. The `dcb-map` command is supported only on physical Ethernet interfaces. To remove a DCB map from an interface, enter the `no dcb-map` *`map-name`* command in Interface configuration mode.
Related Commands	show qos dcb-map– displays the dcb-map profiles configured on the system.

priority-pgid

Assign 802.1p priority traffic to a priority group in a DCB map.

FC Flex IO Modules with MXL

Syntax

```
priority-pgid dot1p0_group-num dot1p1_group-num dot1p2_group-
num dot1p3_group-num dot1p4_group-num dot1p5_group-num
dot1p6_group-num dot1p7_group-num
```

Parameters

dot1p0_group-num *dot1p1_group-num* *dot1p2_group-num* *dot1p3_group-num* *dot1p4_group-num* *dot1p5_group-num* *dot1p6_group-num* *dot1p7_group-num*	Enter the priority group number for each 802.1p class of traffic in a DCB map.

Defaults

None

Command Modes

DCB MAP

Command History

Version 9.3(0.0)	Introduced on the FC Flex IO module installed in the MXL 10/40GbE Switch module platform.

Usage Information

PFC and ETS settings are not pre-configured on Ethernet ports. You must use the `dcb-map` command to configure different groups of 802.1p priorities with PFC and ETS settings.

Using the `priority-pgid` command, you assign each 802.1p priority to one priority group. A priority group consists of 802.1p priority values that are grouped together for similar bandwidth allocation and scheduling, and that share latency and loss requirements. All 802.1p priorities mapped to the same queue must be in the same priority group. For example, the `priority-pgid 0 0 0 1 2 4 4 4` command creates the following groups of 802.1p priority traffic:

- Priority group 0 contains traffic with dot1p priorities 0, 1, and 2.
- Priority group 1 contains traffic with dot1p priority 3.
- Priority group 2 contains traffic with dot1p priority 4.
- Priority group 4 contains traffic with dot1p priority 5, 6, and 7.

To remove a priority-pgid configuration from a DCB map, enter the `no priority-pgid` command.

Related Commands

dcb-map — creates a DCB map to configure PFC and ETS parameters and applies the PFC and ETS settings on Ethernet ports.

priority-group bandwidth pfc— configures the ETS bandwidth allocation and the PFC setting used to manage the port traffic in an 802.1p priority group.

priority-group bandwidth pfc

Configure the ETS bandwidth allocation and PFC mode used to manage port traffic in an 802.1p priority group.

MXL 10/40GbE Switch with the FC Flex IO module

Syntax

```
priority-group group-num {bandwidth percentage| strict-
priority} pfc {on | off}
```

Parameters

priority-group *group-num*	Enter the keyword `priority-group` followed by the number of an 802.1p priority group. Use the `priority-pgid` command to create the priority groups in a DCB map.
bandwidth *percentage*	Enter the keyword `bandwidth` followed by a bandwidth percentage allocated to the priority group. The range of valid values is 1 to 100. The sum of all allocated bandwidth percentages in priority groups in a DCB map must be 100%.

strict-priority	Configure the priority-group traffic to be handled with strict priority scheduling. Strict-priority traffic is serviced first, before bandwidth allocated to other priority groups is made available.
pfc {on | off}	Configure whether priority-based flow control is enabled (on) or disabled (off) for port traffic in the priority group.

Defaults None

Command Modes DCB MAP

Command History

Version 9.3(0.0)	Introduced on the MXL 10/40GbE Switch with the FC Flex IO module.

Usage Information

Use the `dcb-map` command to configure priority groups with PFC and/or ETS settings and apply them to Ethernet interfaces.

Use the `priority-pgid` command to map 802.1p priorities to a priority group. You can assign each 802.1p priority to only one priority group. A priority group consists of 802.1p priority values that are grouped together for similar bandwidth allocation and scheduling, and that share latency and loss requirements. All 802.1p priorities mapped to the same queue must be in the same priority group.

Repeat the `priority-group bandwidth pfc` command to configure PFC and ETS traffic handling for each priority group in a DCB map.

You can enable PFC on a maximum of two priority queues.

If you configure more than one priority group as strict priority, the higher numbered priority queue is given preference when scheduling data traffic.

If a priority group does not use its allocated bandwidth, the unused bandwidth is made available to other priority groups.

To remove a priority-group configuration in a DCB map, enter the `no priority-group bandwidth pfc` command.

By default, equal bandwidth is assigned to each dot1p priority in a priority group. Use the `bandwidth` parameter to configure the bandwidth percentage assigned to a priority group. The sum of the bandwidth allocated to all priority groups in a DCB map must be 100% of the bandwidth on the link. You must allocate at least 1% of the total port bandwidth to each priority group.

Related Commands

dcb-map – creates a DCB map to configure PFC and ETS parameters and applies the PFC and ETS settings on Ethernet ports.

priority-pgid – configures the 802.1p priority traffic in a priority group for a DCB map.

show dcb-map

Display the DCB configuration parameters in DCB maps.

FC Flex IO Modules with MXL

Syntax

```
show dcb-map brief dcb-map-name
```

Parameters

brief	Displays an overview of currently configured DCB maps and the operational status of the ports on which they are applied.
dcb-map-name	Displays the DCB configuration parameters in a specified map that is applied on Ethernet (FCoE) ports.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.3(0.0)	Introduced on the FC Flex IO module installed in the MXL 10/40GbE Switch.

Usage Information

Use the `show dcb-map` command to display the enhanced transmission selection (ETS) and priority-based flow control (PFC) parameters used to configure Ethernet (FCoE) ports in a converged network.

You can also configure and apply a different DCB map with other PFC and ETS settings to customize the handling of CEE traffic on specified ports (`dcb-map` command).

The following table describes the `show dcb-map brief` and `show dcb-map` output shown in the example below.

Field	Description
DCB Map Name	Name of a DCB map.
Interface	Ethernet interface on which DCB map has been applied.
Status	Operational status of the interface: enabled (active) or disabled (not active).
Priority Group	Number of an 802.1p traffic group.
Priorities	802.1p priority traffic assigned to the group.
Bandwidth	Percentage of available bandwidth allocated to the specified group.
PFC-enabled priorities	802.1p priority traffic on which PFC is enabled.

Example

```
Dell# show dcb-map brief
Dcb-map-name  Interface Status
dcbmapABC     te 0/0    Active
dcbmapABC      te 0/1    Active
dcbmapXYZ      te 0/2    Not active

Dell# show dcb-map dcbmapABC
Priority-Group Table:
Priority-Group        Priorities        Bandwidth(%)
0                   0,1,2,5,6,7      50
1                   3                30
2                   4                20
3                   -
5                   -
6                   -
7                   -
PFC Enabled priorities: 3, 4
```

Related Commands

[dcb-map](#) — creates a DCB map to configure DCB parameters on Ethernet ports that support converged Ethernet traffic.

show qos dcb-map

Display the DCB parameters configured in a specified DCB map.

FC Flex IO Modules with MXL

Syntax

`show qos dcb-map *map-name*`

Parameters

map-name	Displays the PFC and ETS parameters configured in the specified map.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.3(0.0)	Introduced on the FC Flex IO module installed in the MXL 10/40GbE Switch.

Usage Information

Use the `show qos dcb-map` command to display the enhanced transmission selection (ETS) and priority-based flow control (PFC) parameters used to configure server-facing Ethernet ports.

The following table describes the `show qos dcb-map` output shown in the example below.

Field	Description
State	Complete: All mandatory DCB parameters are correctly configured. In progress: The DCB map configuration is not complete. Some mandatory parameters are not configured.
PFC Mode	PFC configuration in DCB map: On (enabled) or Off.
PG	Priority group configured in the DCB map.

Field	Description
TSA	Transmission scheduling algorithm used by the priority group: Enhanced Transmission Selection (ETS).
BW	Percentage of bandwidth allocated to the priority group.
PFC	PFC setting for the priority group: On (enabled) or Off.
Priorities	802.1p priorities configured in the priority group.

Example

```
Dell# show qos dcb-map dcbmap2

State   :Complete
PfcMode:ON
--------------------
PG:0 TSA:ETS  BW:50  PFC:OFF
Priorities:0 1 2 4 5 6 7


PG:1 TSA:ETS  BW:50  PFC:ON
Priorities:3
```

Related Commands

dcb-map — creates a DCB map to configure PFC and ETS parameters and applies the PFC and ETS settings on Ethernet ports.

DCB Command

The following DCB command is supported on the FC Flex IO module installed in the MXL 10/40GbE Switch platform.

dcb-enable

Enable data center bridging.

Syntax

`dcb enable`

To disable DCB, use the `no dcb enable` command.

Defaults

none

Command Modes

CONFIGURATION

Command History

Version 9.3(0.0)	Introduced on the FC Flex IO module installed in the MXL 10/40GbE Switch

Usage Information

DCB is not supported if you enable `link-level flow control` on one or more interfaces.

DCBX Commands

The following DCBX commands are supported on the FC Flex IO module installed in the M I/O Aggregator and MXL 10/40GbE Switch platforms.

advertise dcbx-appln-tlv

On a DCBX port with a manual role, configure the application priority TLVs advertised on the interface to DCBX peers.

Syntax

```
advertise dcbx-appln-tlv {fcoe | iscsi}
```

To remove the application priority TLVs, use the `no advertise dcbx-appln-tlv {fcoe | iscsi}` command.

Parameters

{fcoe | iscsi}	Enter the application priority TLVs, where: • `fcoe`: enables the advertisement of FCoE in application priority TLVs. • `iscsi`: enables the advertisement of iSCSI in application priority TLVs.

Defaults

Application priority TLVs are enabled to advertise FCoE and iSCSI.

Command Modes

PROTOCOL LLDP

Command History

Version 9.3.0.0	Introduced on the FC Flex IO module installed in the M I/O Aggregator and MXL 10/40GbE Switch

Usage Information

To disable TLV transmission, use the `no` form of the command; for example, `no advertise dcbx-appln-tlv iscsi`.

advertise dcbx-tlv

On a DCBX port with a manual role, configure the PFC and ETS TLVs advertised to DCBX peers.

Syntax

```
advertise dcbx-tlv {ets-conf | ets-reco | pfc} [ets-conf | ets-reco | pfc] [ets-conf | ets-reco | pfc]
```

To remove the advertised ETS TLVs, use the `no advertise dcbx-tlv` command.

Parameters

{ets-conf | ets-reco | pfc}	Enter the PFC and ETS TLVs advertised, where: • `ets-conf:` enables the advertisement of ETS configuration TLVs. • `ets-reco:` enables the advertisement of ETS recommend TLVs. • `pfc:` enables the advertisement of PFC TLVs.

Defaults	All PFC and ETS TLVs are advertised.
Command Modes	PROTOCOL LLDP
Command History	**Version 9.3.0.0** Introduced on the FC Flex IO module installed in the M I/O Aggregator and MXL 10/40GbE Switch

Usage Information

You can configure the transmission of more than one TLV type at a time; for example: `advertise dcbx-tlv ets-conf ets-reco`.

You can enable ETS recommend TLVs (`ets-reco`) only if you enable ETS configuration TLVs (`ets-conf`). To disable TLV transmission, use the `no` form of the command; for example, `no advertise dcbx-tlv pfc ets-reco`.

DCBX requires that you enable LLDP to advertise DCBX TLVs to peers.

Configure DCBX operation at the INTERFACE level on a switch or globally on the switch. To verify the DCBX configuration on a port, use the `show interface dcbx detail` command.

dcbx port-role

Configure the DCBX port role the interface uses to exchange DCB information.

Syntax

```
dcbx port-role {config-source | auto-downstream | auto-upstream
| manual}
```

To remove DCBX port role, use the `no dcbx port-role {config-source | auto-downstream | auto-upstream | manual}` command.

Parameters

config-source | auto-downstream | auto-upstream | manual	Enter the DCBX port role, where: • `config-source`: configures the port to serve as the configuration source on the switch. • `auto-upstream`: configures the port to receive a peer configuration. The configuration source is elected from auto-upstream ports. • `auto-downstream`: configures the port to accept the internally propagated DCB configuration from a configuration source. • `manual`: configures the port to operate only on administer-configured DCB parameters. The port does not accept a DCB configuration received form a peer or a local configuration source.

Defaults	**Manual**
Command Modes	INTERFACE PROTOCOL LLDP

Command History

Version 9.3.0.0	Introduced on the FC Flex IO module installed in the M I/O Aggregator and MXL 10/40GbE Switch

Usage Information

DCBX requires that you enable LLDP to advertise DCBX TLVs to peers.

Configure DCBX operation at the INTERFACE level on a switch or globally on the switch. To verify the DCBX configuration on a port, use the `show interface dcbx detail` command.

dcbx version

Configure the DCBX version used on the interface.

Syntax

```
dcbx version {auto | cee | cin | ieee-v2.5}
```

To remove the DCBX version, use the `dcbx version {auto | cee | cin | ieee-v2.5}` command.

Parameters

auto | cee | cin | ieee-v2.5	Enter the DCBX version type used on the interface, where: • `auto`: configures the port to operate using the DCBX version received from a peer. • `cee`: configures the port to use CDD (Intel 1.01). • `cin`: configures the port to use Cisco-Intel-Nuova (DCBX 1.0). • `ieee-v2`: configures the port to use IEEE 802.1az (Draft 2.5).

Defaults **Auto**

Command Modes INTERFACE PROTOCOL LLDP

Command History

Version 9.3.0.0	Introduced on the FC Flex IO module installed in the M I/O Aggregator and MXL 10/40GbE Switch

Usage Information

DCBX requires that you enable LLDP to advertise DCBX TLVs to peers.

Configure DCBX operation at the INTERFACE level on a switch or globally on the switch. To verify the DCBX configuration on a port, use the `show interface dcbx detail` command.

debug dcbx

Enable DCBX debugging.

Syntax

```
debug dcbx {all | auto-detect-timer | config-exchng | fail |
mgmt | resource | sem | tlv}
```

To disable DCBX debugging, use the `no debug dcbx` command.

Parameters

{all | auto-detect-timer | config-exchng | fail | mgmt | resource | sem | tlv}	Enter the type of debugging, where: • `all`: enables all DCBX debugging operations. • `auto-detect-timer`: enables traces for DCBX auto-detect timers. • `config-exchng`: enables traces for DCBX configuration exchanges. • `fail`: enables traces for DCBX failures. • `mgmt`: enables traces for DCBX management frames. • `resource`: enables traces for DCBX system resource frames. • `sem`: enables traces for the DCBX state machine. • `tlv`: enables traces for DCBX TLVs.

Defaults none

Command Modes EXEC Privilege

Command History

Version 9.3.0.0	Introduced on the FC Flex IO module installed in the M I/O Aggregator and MXL 10/40GbE Switch

fcoe priority-bits

Configure the FCoE priority advertised for the FCoE protocol in application priority TLVs.

Syntax `fcoe priority-bits` *`priority-bitmap`*

To remove the configured FCoE priority, use the `no fcoe priority-bits` command.

Parameters

priority-bitmap	Enter the priority-bitmap range. The range is from 1 to FF.

Defaults 0x8

Command Modes PROTOCOL LLDP

Command History

Version 9.3.0.0	Introduced on the FC Flex IO module installed in the M I/O Aggregator and MXL 10/40GbE Switch

Usage Information This command is available at the global level only.

iscsi priority-bits

Configure the iSCSI priority advertised for the iSCSI protocol in application priority TLVs.

Syntax	`iscsi priority-bits` *`priority-bitmap`* To remove the configured iSCSI priority, use the `no iscsi priority-bits` command.
Parameters	*priority-bitmap* — Enter the priority-bitmap range. The range is from 1 to FF.
Defaults	0x10
Command Modes	PROTOCOL LLDP
Command History	Version 9.3.0.0 — Introduced on the FC Flex IO module installed in the M I/O Aggregator and MXL 10/40GbE Switch
Usage Information	This command is available at the global level only.

show interface dcbx detail

Displays the DCBX configuration on an interface.

Syntax	`show interface` *`port-type slot/port`* `dcbx detail`
Parameters	*port-type* — Enter the port type. *slot/port* — Enter the slot/port number.
Command Modes	CONFIGURATION
Command History	Version 9.3.0.0 — Introduced on the FC Flex IO module installed in the M I/O Aggregator and MXL 10/40GbE Switch.
Usage Information	To clear DCBX frame counters, use the `clear dcbx counters interface` *`stack-unit/port`* command. The following describes the `show interface dcbx detail` command shown in the following example.

Field	Description
Interface	Interface type with chassis slot and port number.
Port-Role	Configured the DCBX port role: auto-upstream, auto-downstream, config-source, or manual.

Field	Description
DCBX Operational Status	Operational status (enabled or disabled) used to elect a configuration source and internally propagate a DCB configuration. The DCBX operational status is the combination of PFC and ETS operational status.
Configuration Source	Specifies whether the port serves as the DCBX configuration source on the switch: true (yes) or false (no).
Local DCBX Compatibility mode	DCBX version accepted in a DCB configuration as compatible. In auto-upstream mode, a port can only receive a DCBX version supported on the remote peer.
Local DCBX Configured mode	DCBX version configured on the port: CEE, CIN, IEEE v2.5, or Auto (port auto-configures to use the DCBX version received from a peer).
Peer Operating version	DCBX version that the peer uses to exchange DCB parameters.
Local DCBX TLVs Transmitted	Transmission status (enabled or disabled) of advertised DCB TLVs (see TLV code at the top of the show command output).
Local DCBX Status: DCBX Operational Version	DCBX version advertised in Control TLVs.
Local DCBX Status: DCBX Max Version Supported	Highest DCBX version supported in Control TLVs.
Local DCBX Status: Sequence Number	Sequence number transmitted in Control TLVs.
Local DCBX Status: Acknowledgment Number	Acknowledgement number transmitted in Control TLVs.
Local DCBX Status: Protocol State	Current operational state of the DCBX protocol: ACK or IN-SYNC.
Peer DCBX Status: DCBX Operational Version	DCBX version advertised in Control TLVs received from the peer device.
Peer DCBX Status: DCBX Max Version Supported	Highest DCBX version supported in Control TLVs received from the peer device.

Field	Description
Peer DCBX Status: Sequence Number	Sequence number transmitted in Control TLVs received from the peer device.
Peer DCBX Status: Acknowledgment Number	Acknowledgement number transmitted in Control TLVs received from the peer device.
Total DCBX Frames transmitted	Number of DCBX frames sent from the local port.
Total DCBX Frames received	Number of DCBX frames received from the remote peer port.
Total DCBX Frame errors	Number of DCBX frames with errors received.
Total DCBX Frames unrecognized	Number of unrecognizable DCBX frames received.

Example

```
Dell(conf)# show interface tengigabitethernet 0/49 dcbx detail
Dell#show interface te 0/49 dcbx detail

E-ETS Configuration TLV enabled
  e-ETS Configuration TLV disabled
R-ETS Recommendation TLV enabled
  r-ETS Recommendation TLV disabled
P-PFC Configuration TLV enabled
  p-PFC Configuration TLV disabled
F-Application priority for FCOE enabled
  f-Application Priority for FCOE disabled
I-Application priority for iSCSI enabled
  i-Application Priority for iSCSI disabled
-----------------------------------------------------------

Interface TenGigabitEthernet 0/49
  Remote Mac Address 00:00:00:00:00:11
   Port Role is Auto-Upstream
  DCBX Operational Status is Enabled
  Is Configuration Source? TRUE

Local DCBX Compatibility mode is CEE
  Local DCBX Configured mode is CEE
  Peer Operating version is CEE
  Local DCBX TLVs Transmitted: ErPfi

Local DCBX Status
-----------------
  DCBX Operational Version is 0
  DCBX Max Version Supported is 0
  Sequence Number: 2
  Acknowledgment Number: 2
  Protocol State: In-Sync

Peer DCBX Status:
----------------
  DCBX Operational Version is 0
DCBX Max Version Supported is 255
Sequence Number: 2
Acknowledgment Number: 2
Total DCBX Frames transmitted 27
Total DCBX Frames received 6
Total DCBX Frame errors 0
Total DCBX Frames unrecognized 0
```

ETS Commands

The following ETS commands are supported on the FC Flex IO module installed in the MXL 10/40GbE Switch platform.

bandwidth-percentage

Configure the bandwidth percentage allocated to priority traffic in port queues.

Syntax

`bandwidth-percentage` *`percentage`*

To remove the configured bandwidth percentage, use the `no bandwidth-percentage` command.

Parameters

percentage	(Optional) Enter the bandwidth percentage. The percentage range is from 1 to 100% in units of 1%.

Defaults

none

Command Modes

QOS-POLICY-OUT-ETS

Command History

Version 9.3(0.0)	Introduced on the FC Flex IO module installed in the MXL 10/40GbE Switch.

Usage Information

By default, equal bandwidth is assigned to each port queue and each dot1p priority in a priority group. To configure bandwidth amounts in associated dot1p queues, use the `bandwidth-percentage` command. When specified bandwidth is assigned to some port queues and not to others, the remaining bandwidth (100% minus assigned bandwidth amount) is equally distributed to unassigned non-strict priority queues in the priority group. The sum of the allocated bandwidth to all queues in a priority group must be 100% of the bandwidth on the link.

ETS-assigned bandwidth allocation applies only to data queues, not to control queues.

The configuration of bandwidth allocation and strict-queue scheduling is not supported at the same time for a priority group. If you configure both, the configured bandwidth allocation is ignored for priority-group traffic when you apply the output policy on an interface.

By default, equal bandwidth is assigned to each priority group in the ETS output policy applied to an egress port if you did not configure bandwidth allocation. The sum of configured bandwidth allocation to dot1p priority traffic in all ETS priority groups must be 100%. Allocate at least 1% of the total bandwidth to each priority group and queue. If bandwidth is assigned to some priority groups but not to others, the remaining bandwidth (100% minus assigned bandwidth amount) is equally distributed to nonstrict-priority groups which have no configured scheduler.

Related Commands	- qos-policy-output ets — creates a QoS output policy. - scheduler — schedules priority traffic in port queues.

clear ets counters

Clear all ETS TLV counters on an interface.

Syntax	`clear ets counters port-type slot/port`
Parameters	**port-type**: Enter the keywords `port-type` then the slot/port information.
Defaults	none
Command Modes	EXEC Privilege
Command History	**Version 9.3(0.0)**: Introduced on the FC Flex IO module installed in the MXL 10/40GbE Switch.

dcb-map

Create a DCB map to configure priority flow control (PFC) and enhanced transmission selection (ETS) on Ethernet ports that support converged Ethernet traffic. Apply the DCB map to an Ethernet interface.

Syntax	`dcb-map map-name`
Parameters	***map-name***: Enter a DCB map name. The maximum number of alphanumeric characters is 32.
Defaults	None.
Command Modes	CONFIGURATION INTERFACE
Command History	**Version 9.3(0.0)**: Introduced on the FC Flex IO module installed in the MXL 10/40GbE Switch.

Usage Information	A DCB map is a template used to configure DCB parameters and apply them on converged Ethernet interfaces. DCB parameters include priority-based flow control (PFC) and enhanced traffic selection (ETS). To display the PFC and ETS settings in DCB maps, enter the `show qos dcb-map` command. Use the `dcb-map` command to create a DCB map to specify PFC and ETS settings and apply it on Ethernet ports. After you apply a DCB map to an interface, the PFC and ETS settings in the map are applied when the Ethernet port is enabled. DCBx is enabled on Ethernet ports by default. The `dcb-map` command is supported only on physical Ethernet interfaces. To remove a DCB map from an interface, enter the `no dcb-map` *`map-name`* command in Interface configuration mode.
Related Commands	show qos dcb-map– displays the dcb-map profiles configured on the system.

priority-group bandwidth pfc

Configure the ETS bandwidth allocation and PFC mode used to manage port traffic in an 802.1p priority group.

MXL 10/40GbE Switch with the FC Flex IO module

Syntax

```
priority-group group-num {bandwidth percentage| strict-priority} pfc {on | off}
```

Parameters

priority-group *group-num*	Enter the keyword `priority-group` followed by the number of an 802.1p priority group. Use the `priority-pgid` command to create the priority groups in a DCB map.
bandwidth *percentage*	Enter the keyword `bandwidth` followed by a bandwidth percentage allocated to the priority group. The range of valid values is 1 to 100. The sum of all allocated bandwidth percentages in priority groups in a DCB map must be 100%.
strict-priority	Configure the priority-group traffic to be handled with strict priority scheduling. Strict-priority traffic is serviced first, before bandwidth allocated to other priority groups is made available.
pfc {on | off}	Configure whether priority-based flow control is enabled (on) or disabled (off) for port traffic in the priority group.

Defaults	None
Command Modes	DCB MAP

Command History	**Version 9.3(0.0)**	Introduced on the MXL 10/40GbE Switch with the FC Flex IO module.

Usage Information

Use the `dcb-map` command to configure priority groups with PFC and/or ETS settings and apply them to Ethernet interfaces.

Use the `priority-pgid` command to map 802.1p priorities to a priority group. You can assign each 802.1p priority to only one priority group. A priority group consists of 802.1p priority values that are grouped together for similar bandwidth allocation and scheduling, and that share latency and loss requirements. All 802.1p priorities mapped to the same queue must be in the same priority group.

Repeat the `priority-group bandwidth pfc` command to configure PFC and ETS traffic handling for each priority group in a DCB map.

You can enable PFC on a maximum of two priority queues.

If you configure more than one priority group as strict priority, the higher numbered priority queue is given preference when scheduling data traffic.

If a priority group does not use its allocated bandwidth, the unused bandwidth is made available to other priority groups.

To remove a priority-group configuration in a DCB map, enter the `no priority-group bandwidth pfc` command.

By default, equal bandwidth is assigned to each dot1p priority in a priority group. Use the `bandwidth` parameter to configure the bandwidth percentage assigned to a priority group. The sum of the bandwidth allocated to all priority groups in a DCB map must be 100% of the bandwidth on the link. You must allocate at least 1% of the total port bandwidth to each priority group.

Related Commands

dcb-map – creates a DCB map to configure PFC and ETS parameters and applies the PFC and ETS settings on Ethernet ports.

priority-pgid – configures the 802.1p priority traffic in a priority group for a DCB map.

scheduler

Configure the method used to schedule priority traffic in port queues.

Syntax

`scheduler value`

To remove the configured priority schedule, use the `no scheduler` command.

Parameters

value	Enter schedule priority value. The valid values are: • `strict`: strict-priority traffic is serviced before any other queued traffic.

- `werr`: weighted elastic round robin (werr) provides low-latency scheduling for priority traffic on port queues.

Defaults

Weighted elastic round robin (WERR) scheduling is used to queue priority traffic.

Command Modes

POLICY-MAP-OUT-ETS

Command History

Version 9.3(0.0)	Introduced on the FC Flex IO module installed in the M I/O Aggregator and MXL 10/40GbE Switch.

Usage Information

dot1p priority traffic on the switch is scheduled to the current queue mapping. dot1p priorities within the same queue must have the same traffic properties and scheduling method.

ETS-assigned scheduling applies only to data queues, not to control queues.

The configuration of bandwidth allocation and strict-queue scheduling is not supported at the same time for a priority group. If you configure both, the configured bandwidth allocation is ignored for priority-group traffic when you apply the output policy on an interface.

Related Commands

- qos-policy-output ets — configures the ETS bandwidth allocation.
- bandwidth-percentage — bandwidth percentage allocated to priority traffic in port queues.

set-pgid

Configure the priority-group identifier.

Syntax

`set-pgid` *`value`*

To remove the priority group, use the `no set-pgid` command.

Parameters

value	Enter the priority group identification. The range is from 0 to 7.

Defaults

none

Command Modes

PRIORITY-GROUP

Command History

Version 9.3.0.0	Introduced on the FC Flex IO module installed in the M I/O Aggregator and MXL 10/40GbE Switch.

Related Commands

- priority-group qos-policy — creates an ETS priority group.
- priority-list — configures the 802.1p priorities.

show interface ets

Displays the ETS configuration applied to egress traffic on an interface, including priority groups with priorities and bandwidth allocation.

Syntax `show interface port-type slot/port ets {summary | detail}`

Parameters

port-type slot/ port ets	Enter the port-type slot and port ETS information.
{summary | detail}	Enter the keyword `summary` for a summary list of results or enter the keyword `detail` for a full list of results.

Command Modes CONFIGURATION

Command History

Version 9.3.0.0	Introduced on the FC Flex IO module installed in the M I/O Aggregator and MXL 10/40GbE Switch.

Usage Information

To clear ETS TLV counters, use the `clear ets counters interface port-type slot/port` command.

The following describes the `show interface summary` command shown in the following example.

Field	Description
Interface	Interface type with stack-unit and port number.
Max Supported TC Group	Maximum number of priority groups supported.
Number of Traffic Classes	Number of 802.1p priorities currently configured.
Admin mode	ETS mode: on or off. When on, the scheduling and bandwidth allocation configured in an ETS output policy or received in a DCBX TLV from a peer can take effect on an interface.
Admin Parameters	ETS configuration on local port, including priority groups, assigned dot1p priorities, and bandwidth allocation.
Remote Parameters	ETS configuration on remote peer port, including admin mode (enabled if a valid TLV was received or disabled), priority groups, assigned dot1p priorities, and bandwidth allocation. If ETS admin mode is enabled on the remote port for DCBX exchange, the Willing bit received in ETS TLVs from the remote peer is included.

Field	Description
Local Parameters	ETS configuration on local port, including admin mode (enabled when a valid TLV is received from a peer), priority groups, assigned dot1p priorities, and bandwidth allocation.
Operational status (local port)	Port state for current operational ETS configuration: • `Init`: Local ETS configuration parameters were exchanged with the peer. • `Recommend`: Remote ETS configuration parameters were received from the peer. • `Internally propagated`: ETS configuration parameters were received from the configuration source.
ETS DCBX Oper status	Operational status of the ETS configuration on the local port: match or mismatch.
State Machine Type	Type of state machine used for DCBX exchanges of ETS parameters: Feature — for legacy DCBX versions; Asymmetric — for an IEEE version.
Conf TLV Tx Status	Status of ETS Configuration TLV advertisements: enabled or disabled.
Reco TLV Tx Status	Status of ETS Recommendation TLV advertisements: enabled or disabled.
Input Conf TLV pkts	Number of ETS Configuration TLVs received.
Output Conf TLV pkts	Number of ETS Configuration TLVs transmitted.
Error Conf TLV pkts	Number of ETS Error Configuration TLVs received.
Input Reco TLV pkts	Number of ETS Recommendation TLVs received.
Output Reco TLV pkts	Number of ETS Recommendation TLVs transmitted.
Error Reco TLV pkts	Number of ETS Error Recommendation TLVs received.

Example (Summary)

```
Dell(conf)# show interfaces te 0/0 ets summary
Interface TenGigabitEthernet 0/0
Max Supported TC Groups is 4
Number of Traffic Classes is 8
Admin mode is on
Admin Parameters:
------------------
Admin is enabled
TC-grp Priority#        Bandwidth TSA
0      0,1,2,3,4,5,6,7  100%      ETS
```

```
1                         0%      ETS
2                         0%      ETS
3                         0%      ETS
4                         0%      ETS
5                         0%      ETS
6                         0%      ETS
7                         0%      ETS
Priority#              Bandwidth  TSA
0                        13%      ETS
1                        13%      ETS
2                        13%      ETS
3                        13%      ETS
4                        12%      ETS
5                        12%      ETS
6                        12%      ETS
7                        12%      ETS
Remote Parameters:
-------------------
Remote is disabled
Local Parameters:
------------------
Local is enabled
TC-grp Priority#        Bandwidth TSA
0      0,1,2,3,4,5,6,7  100%      ETS
1                         0%      ETS
2                         0%      ETS
3                         0%      ETS
4                         0%      ETS
5                         0%      ETS
6                         0%      ETS
7                         0%      ETS
Priority#               Bandwidth TSA
0                        13%      ETS
1                        13%      ETS
2                        13%      ETS
3                        13%      ETS
4                        12%      ETS
5                        12%      ETS
6                        12%      ETS
7                        12%      ETS
Oper status is init
Conf TLV Tx Status is disabled
Traffic Class TLV Tx Status is disabled
```

Example (Detail)

```
Dell(conf)# show interfaces tengigabitethernet 0/0 ets detail
Interface TenGigabitEthernet 0/0
Max Supported TC Groups is 4
Number of Traffic Classes is 8
Admin mode is on
Admin Parameters :
------------------
Admin is enabled
TC-grp Priority#        Bandwidth TSA
0      0,1,2,3,4,5,6,7  100%      ETS
1                       0%        ETS
2                       0%        ETS
3                       0%        ETS
4                       0%        ETS
5                       0%        ETS
6                       0%        ETS
7                       0%        ETS

Priority#               Bandwidth TSA
```

```
0                        13%       ETS
1                        13%       ETS
2                        13%       ETS
3                        13%       ETS
4                        12%       ETS
5                        12%       ETS
6                        12%       ETS
7                        12%       ETS
Remote Parameters:
-------------------
Remote is disabled

Local Parameters :
------------------
Local is enabled
TC-grp Priority#         Bandwidth TSA
0      0,1,2,3,4,5,6,7  100%      ETS
1                        0%        ETS
2                        0%        ETS
3                        0%        ETS
4                        0%        ETS
5                        0%        ETS
6                        0%        ETS
7                        0%        ETS

Priority#                Bandwidth TSA
0                        13%       ETS
1                        13%       ETS
2                        13%       ETS
3                        13%       ETS
4                        12%       ETS
5                        12%       ETS
6                        12%       ETS
7                        12%       ETS
Oper status is init
Conf TLV Tx Status is disabled
Traffic Class TLV Tx Status is disabled
0 Input Conf TLV Pkts, 0 Output Conf TLV Pkts, 0 Error Conf
TLV Pkts
0 Input Traffic Class TLV Pkts, 0 Output Traffic Class TLV
Pkts, 0 Error Traffic Class
TLV
Pkts
```

show qos dcb-output

Displays the ETS configuration in a DCB output policy.

Syntax `show qos dcb-output [ets-profile]`

Parameters

[ets-profile]	Enter the ETS profile.

Command Modes EXEC Privilege

Command History

Version 9.3.0.0	Introduced on the FC Flex IO module installed in the M I/O Aggregator and MXL 10/40GbE Switch.

Example

```
Dell# show qos dcb-output
dcb-output ets
  priority-group san qos-policy san
  priority-group ipc qos-policy ipc
  priority-group lan qos-policy lan
```

show qos priority-groups

Displays the ETS priority groups configured on the switch, including the 802.1p priority classes and ID of each group.

Syntax `show qos priority-groups`

Command Modes EXEC Privilege

Command History

Version 9.3.0.0	Introduced on the FC Flex IO module installed in the M I/O Aggregator and MXL 10/40GbE Switch.

Example

```
Dell#show qos priority-groups
priority-group ipc
  priority-list 4
  set-pgid 2
```

show stack-unit stack-ports ets details

Displays the ETS configuration applied to egress traffic on stacked ports, including ETS Operational mode on each unit and the configurated priority groups with dot1p priorities, bandwidth allocation, and scheduler type.

Syntax `show stack-unit {all | *stack-unit*} stack-ports {all | *port-number*} ets details`

Parameters

stack-unit	Enter the stack unit identification.
port-number	Enter the port number.

Command Modes CONFIGURATION

Command History

Version 9.3.0.0	Introduced on the FC Flex IO module installed in the M I/O Aggregator and MXL 10/40GbE Switch.

Example

```
Dell(conf)# show stack-unit all stack-ports all ets details

Stack unit 0 stack port all
Max Supported TC Groups is 4
Number of Traffic Classes is 1
Admin mode is on

Admin Parameters:
--------------------
Admin is enabled
TC-grp Priority#        Bandwidth TSA
```

```
------------------------------------------------
0      0,1,2,3,4,5,6,7  100%      ETS
1                       - -
2                       - -
3                       - -
4                       - -
5                       - -
6                       - -
7                       - -
8                       - -

Stack unit 1 stack port all
Max Supported TC Groups is 4
Number of Traffic Classes is 1
Admin mode is on
Admin Parameters:
--------------------
Admin is enabled
TC-grp Priority#        Bandwidth TSA
------------------------------------------------
0      0,1,2,3,4,5,6,7  100%      ETS
1                       -         -
2                       -         -
3                       -         -
4                       -         -
5                       -         -
6                       -         -
7                       -         -
8                       -         -
```

PFC Commands

The following PFC commands are supported on the FC Flex IO module installed in the MXL 10/40GbE Switch platform.

clear pfc counters

Clear the PFC TLV counters and PFC statistics on an interface or stack unit.

Syntax

`clear pfc counters [port-type slot/port | stack-unit {`*`unit number`*` | all } all stack-ports all}] | interface {statistics}]`

Parameters

port-type	Enter the keywords `port-type` then the slot/port information.
stack-unit *unit number*	Enter the keywords `stack-unit` then the stack-unit number to be cleared.
all stack-ports all	Enter the keywords `all stack-ports all` to clear the counters on all interfaces.
statistics	Enter the keyword `statistics` to clear only the hardware PFC counters.

Defaults

none

Command Modes	EXEC Privilege
Command History	**Version 9.3(0.0)** Introduced on the FC Flex IO module installed in the MXL 10/40GbE Switch.
Usage Information	If you do not use the `statistics` parameter, both hardware and DCBx counters clear.

description

Enter a text description of the DCB policy (PFC input or ETS output).

Syntax

`description text`

To remove the text description, use the `no description` command.

Parameters

text	Enter the description of the output policy. The maximum is 32 characters.

Defaults: none

Command Modes

- DCB INPUT POLICY
- DCB OUTPUT POLICY

Command History

Version 9.3(0.0)	Introduced on the FC Flex IO module installed in the MXL 10/40GbE Switch.

pfc link-delay

Configure the link delay used to pause specified priority traffic.

Syntax

`pfc link-delay value`

To remove the link delay, use the `no pfc link-delay` command.

Parameters

value	The range is (in quanta) from 712 to 65535. One quantum is equal to a 512-bit transmission.

Defaults: **45556** quantum

Command Modes: DCB INPUT POLICY

Command History

Version 9.3(0.0)	Introduced on the MXL 10/40GbE Switch with the FC Flex IO module.

Usage Information	The minimum link delay must be greater than the round-trip transmission time a peer must honor a PFC pause frame multiplied by the number of PFC-enabled ingress ports.
Related Commands	dcb-input — creates a DCB input policy.

pfc mode on

Enable the PFC configuration on the port so that the priorities are included in DCBX negotiation with peer PFC devices.

Syntax

```
pfc mode on
```

To disable the PFC configuration, use the `no pfc mode on` command.

Defaults	PFC mode is on.
Command Modes	DCB MAP

Command History

Version 9.3(0.0)	Introduced on the MXL 10/40GbE Switch with the FC Flex IO module.

Usage Information

By applying a DCB input policy with PFC enabled, you enable PFC operation on ingress port traffic. To achieve complete lossless handling of traffic, also enable PFC on all DCB egress ports or configure the dot1p priority-queue assignment of PFC priorities to lossless queues (refer to `pfc no-drop queues`).

To disable PFC operation on an interface, enter the `no pfc mode on` command in DCB Input Policy Configuration mode. PFC is enabled and disabled as global DCB operation is enabled (`dcb-enable`) or disabled (`no dcb-enable`).

You cannot enable PFC and link-level flow control at the same time on an interface.

pfc no-drop queues

Configure the port queues that still function as no-drop queues for lossless traffic.

Syntax

```
pfc no-drop queues queue-range
```

To remove the no-drop port queues, use the `no pfc no-drop queues` command.

Parameters

queue-range	Enter the queue range. Separate the queue values with a comma; specify a priority range with a dash; for example, `pfc no-drop queues 1,3` or `pfc no-drop queues 2-3`. The range is from 0 to 3.

Defaults	No lossless queues are configured.
Command Modes	INTERFACE
Command History	Version 9.3(0.0) — Introduced on the MXL 10/40GbE Switch with the FC Flex IO module.

Usage Information

The maximum number of lossless queues globally supported on the switch is two.

- The following lists the dot1p priority-queue assignments.

dot1p Value in the Incoming Frame	Description heading
0	0
1	0
2	0
3	1
4	2
5	3
6	3
7	3

pfc priority

Configure the CoS traffic to be stopped for the specified delay.

Syntax

`pfc priority priority-range`

To delete the pfc priority configuration, use the `no pfc priority` command.

Parameters

priority-range	Enter the 802.1p values of the frames to be paused. Separate the priority values with a comma; specify a priority range with a dash; for example, pfc priority 1,3,5-7. The range is from 0 to 7.

Defaults	none
Command Modes	DCB INPUT POLICY
Command History	Version 9.3(0.0) — Introduced on the MXL 10/40GbE Switch with the FC Flex IO module.

Usage Information	You can enable any number of 802.1p priorities for PFC. Queues to which PFC priority traffic is mapped are lossless by default. Traffic may be interrupted due to an interface flap (going down and coming up) when you reconfigure the lossless queues for no-drop priorities in a PFC input policy and reapply the policy to an interface. The maximum number of lossless queues supported on the switch is two. A PFC peer must support the configured priority traffic (as DCBX detects) to apply PFC.
Related Commands	dcb-input — creates a DCB input policy.

show dcb

Displays the data center bridging status, the number of PFC-enabled ports, and the number of PFC-enabled queues.

Syntax

```
show dcb [stack-unit unit-number]
```

Parameters

unit number	Enter the DCB unit number. The range is from 0 to 5.

Command Modes: EXEC Privilege

Command History

Version 9.3(0.0)	Introduced on the FC Flex IO module installed in the MXL 10/40GbE Switch.

Usage Information: Specify a stack-unit number on the Master switch in a stack.

Example

```
Dell# show dcb
stack-unit 0 port-set 0
      DCB Status : Enabled
    PFC Port Count : 56 (current), 56 (configured)
PFC Queue Count : 2 (current), 2 (configured)
```

show interface pfc

Displays the PFC configuration applied to ingress traffic on an interface, including priorities and link delay.

Syntax

```
show interface port-type slot/port pfc {summary | detail}
```

Parameters

port-type slot/ port pfc	Enter the port-type slot and port PFC information.
{summary | detail}	Enter the keyword `summary` for a summary list of results or enter the keyword `detail` for a full list of results.

Command Modes	INTERFACE
Command History	**Version 9.3(0.0)** Introduced on the FC Flex IO module installed in the MXL 10/40GbE Switch.
Usage Information	To clear the PFC TLV counters, use the `clear pfc counters interface` *`port-type slot/port`* command. The following describes the `show interface pfc summary` command shown in the following example.

Field	Description
Interface	Interface type with stack-unit and port number.
Admin mode is on Admin is enabled	PFC admin mode is on or off with a list of the configured PFC priorities. When the PFC admin mode is on, PFC advertisements are enabled to be sent and received from peers; received PFC configuration take effect. The admin operational status for a DCBX exchange of PFC configuration is enabled or disabled.
Remote is enabled, Priority list Remote Willing Status is enabled	Operational status (enabled or disabled) of peer device for DCBX exchange of PFC configuration with a list of the configured PFC priorities. Willing status of peer device for DCBX exchange (Willing bit received in PFC TLV): enabled or disable.
Local is enabled	DCBX operational status (enabled or disabled) with a list of the configured PFC priorities.
Operational status (local port)	Port state for current operational PFC configuration: • `Init`: Local PFC configuration parameters were exchanged with the peer. • `Recommend`: Remote PFC configuration parameters were received from the peer. • `Internally propagated`: PFC configuration parameters were received from the configuration source.
PFC DCBX Oper status	Operational status for the exchange of the PFC configuration on the local port: match (up) or mismatch (down).
State Machine Type	Type of state machine used for DCBX exchanges of the PFC parameters: Feature — for legacy DCBX versions; Symmetric — for an IEEE version.
TLV Tx Status	Status of the PFC TLV advertisements: enabled or disabled.
PFC Link Delay	Link delay (in quanta) used to pause specified priority traffic.

Field	Description
Application Priority TLV: FCOE TLV Tx Status	Status of FCoE advertisements in application priority TLVs from the local DCBX port: enabled or disabled.
Application Priority TLV: SCSI TLV Tx Status	Status of ISCSI advertisements in application priority TLVs from the local DCBX port: enabled or disabled.
Application Priority TLV: Local FCOE Priority Map	Priority bitmap the local DCBX port uses in FCoE advertisements in application priority TLVs.
Application Priority TLV: Local ISCSI Priority Map	Priority bitmap the local DCBX port uses in ISCSI advertisements in application priority TLVs.
Application Priority TLV: Remote FCOE Priority Map	Status of FCoE advertisements in application priority TLVs from the remote peer port: enabled or disabled.
Application Priority TLV: Remote ISCSI Priority Map	Status of iSCSI advertisements in application priority TLVs from the remote peer port: enabled or disabled.
PFC TLV Statistics: Input TLV pkts	Number of PFC TLVs received.
PFC TLV Statistics: Output TLV pkts	Number of PFC TLVs transmitted.
PFC TLV Statistics: Error pkts	Number of PFC error packets received.
PFC TLV Statistics: Pause Tx pkts	Number of PFC pause frames transmitted.
PFC TLV Statistics: Pause Rx pkts	Number of PFC pause frames received.

Example (Summary)

```
Dell# show interfaces tengigabitethernet 0/49 pfc summary
Interface TenGigabitEthernet 0/49
  Admin mode is on
  Admin is enabled
  Remote is enabled, Priority list is 4
  Remote Willing Status is enabled
  Local is enabled
  Oper status is Recommended
  PFC DCBX Oper status is Up
  State Machine Type is Feature
  TLV Tx Status is enabled
  PFC Link Delay 45556 pause quantams
  Application Priority TLV Parameters :
  --------------------------------------
  FCOE TLV Tx Status is disabled
  ISCSI TLV Tx Status is disabled
  Local FCOE PriorityMap is 0x8
  Local ISCSI PriorityMap is 0x10
  Remote FCOE PriorityMap is 0x8
  Remote ISCSI PriorityMap is 0x8

Dell# show interfaces tengigabitethernet 0/49 pfc detail
  Interface TenGigabitEthernet 0/49
  Admin mode is on
  Admin is enabled
  Remote is enabled
  Remote Willing Status is enabled
  Local is enabled
  Oper status is recommended
  PFC DCBX Oper status is Up
  State Machine Type is Feature
  TLV Tx Status is enabled
  PFC Link Delay 45556 pause quanta
  Application Priority TLV Parameters :
  --------------------------------------
  FCOE TLV Tx Status is disabled
  ISCSI TLV Tx Status is disabled
  Local FCOE PriorityMap is 0x8
  Local ISCSI PriorityMap is 0x10
  Remote FCOE PriorityMap is 0x8
  Remote ISCSI PriorityMap is 0x8
  0 Input TLV pkts, 1 Output TLV pkts, 0 Error pkts,
  0 Pause Tx pkts, 0 Pause Rx pkts
```

show interface pfc statistics

Displays counters for the PFC frames received and transmitted (by dot1p priority class) on an interface.

Syntax

`show interface port-type slot/port pfc statistics`

Parameters

port-type	Enter the port type.
slot/port	Enter the slot/port number.

Command Modes

INTERFACE

Command History

Version 9.3(0.0)	Introduced on the FC Flex IO module installed in the MXL 10/40GbE Switch.

Example (Summary)

```
Dell#show interfaces te 0/3 pfc statistics
Interface TenGigabitEthernet 0/3

Priority Rx XOFF Frames Rx Total Frames Tx Total Frames
-------------------------------------------------------
0        0              0               0
1        0              0               0
2        0              0               0
3        0              0               0
4        0              0               0
5        0              0               0
```

```
6         0               0                0
7         0               0                0
```

show qos dcb-input

Displays the PFC configuration in a DCB input policy.

Syntax `show qos dcb-input [pfc-profile]`

Parameters

pfc-profile	Enter the PFC profile.

Command Modes CONFIGURATION

Command History

Version 9.3(0.0)	Introduced on the FC Flex IO module installed in the MXL 10/40GbE Switch.

Example

```
Dell(conf)# show qos dcb-input
dcb-input pfc-profile
  pfc link-delay 32
  pfc priority 0-1
dcb-input pfc-profile1
  no pfc mode on
  pfc priority 6-7
```

show stack-unit stack-ports pfc details

Displays the PFC configuration applied to ingress traffic on stacked ports, including PFC Operational mode on each unit with the configured priorities, link delay, and number of pause packets sent and received.

Syntax `show stack-unit {all | stack-unit} stack-ports {all | port-number} pfc details`

Parameters

stack-unit	Enter the stack unit.
port-number	Enter the port number.

Command Modes CONFIGURATION

Command History

Version 9.3(0.0)	Introduced on the FC Flex IO module installed in the MXL 10/40GbE Switch.

Example

```
Dell(conf)# show stack-unit all stack-ports all pfc details

stack unit 0 stack-port all
  Admin mode is On
  Admin is enabled, Priority list is 4-5
  Local is enabled, Priority list is 4-5
  Link Delay 45556 pause quantum
  0 Pause Tx pkts, 0 Pause Rx pkts
```

```
stack unit 1 stack-port all
  Admin mode is On
  Admin is enabled, Priority list is 4-5
  Local is enabled, Priority list is 4-5
  Link Delay 45556 pause quantum
  0 Pause Tx pkts, 0 Pause Rx pkts
```

Fibre Channel over Ethernet for FC Flex IO Modules

FCoE provides a converged Ethernet network that allows the combination of storage-area network (SAN) and LAN traffic on a Layer 2 link by encapsulating Fibre Channel data into Ethernet frames.

The Fibre Channel (FC) Flex IO module is supported on Dell Networking Operating System (OS) MXL 10/40GbE Switch and M I/O Aggregator (IOA). The MXL and IOA switch installed with the FC Flex IO module functions as a top-of-rack edge switch that supports converged enhanced Ethernet (CEE) traffic — Fibre channel over Ethernet (FCoE) for storage, Interprocess Communication (IPC) for servers, and Ethernet local area network (LAN) (IP cloud) for data — as well as FC links to one or more storage area network (SAN) fabrics.

FCoE works with the Ethernet enhancements provided in Data Center Bridging (DCB) to support lossless (no-drop) SAN and LAN traffic. In addition, DCB provides flexible bandwidth sharing for different traffic types, such as LAN and SAN, according to 802.1p priority classes of service. DCBx should be enabled on the system before the FIP snooping feature is enabled.

All of the commands that are supported for FCoE on the MXL and I/O Aggregator apply to the FC Flex IO modules. Similarly, all of the configuration procedures and the settings that are applicable for FCoE on the MXL and I/O Aggregator are valid for the FC Flex IO modules.

Legacy FIP snooping-related commands are supported on 10G optional modules when the Fiber channel capability is disabled (by using the `no feature fc` command). If the FC capability is enabled, only the `fip-snooping max-sessions-per-enodemac` command is supported and the remaining FIP snooping commands are not supported.

NPIV Proxy Gateway for FC Flex IO Modules

The N-port identifier virtualization (NPIV) Proxy Gateway (NPG) feature provides FCoE-FC bridging capability on the M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module switch, allowing server CNAs to communicate with SAN fabrics over the M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module.

To configure the M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module to operate as an NPIV proxy gateway, use the following commands:

dcb-map

Create a DCB map to configure priority flow control (PFC) and enhanced transmission selection (ETS) on Ethernet ports that support converged Ethernet traffic. Apply the DCB map to an Ethernet interface.

M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module

Syntax `dcb-map map-name`

Parameters

map-name	Enter a DCB map name. The maximum number of alphanumeric characters is 32.

Defaults None. There are no pre-configured PFC and ETS settings on M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module Ethernet interfaces. With auto-detection of DCB enabled, a DCB map named 'dcb-map' is applied on all the Ethernet interfaces on which the DCBx frames are observed.

Command Modes

CONFIGURATION

INTERFACE

Command History

Version 9.3(0.0)	Introduced on the M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module.

Usage Information

A DCB map is a template used to configure DCB parameters and apply them on converged Ethernet interfaces. DCB parameters include priority-based flow control (PFC) and enhanced traffic selection (ETS).

To display the PFC and ETS settings in DCB maps, enter the `show qos dcb-map` command.

Use the `dcb-map` command to create a DCB map to specify PFC and ETS settings and apply it on Ethernet ports. After you apply a DCB map to an interface, the PFC and ETS settings in the map are applied when the Ethernet port is enabled. DCBx is enabled on Ethernet ports by default.

The `dcb-map` command is supported only on physical Ethernet interfaces.

To remove a DCB map from an interface, enter the `no dcb-map map-name` command in Interface configuration mode.

Related Commands

show qos dcb-map– displays the dcb-map profiles configured on the system.

description (for FCoE maps)

In an FCoE map, add a text description of the FCoE and FC parameters used to transmit storage traffic over an M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module NPIV proxy gateway in a converged fabric.

M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module

Syntax `description text`

Parameters

text	Enter a maximum of 32 characters.

Defaults None

Command Modes FCOE MAP

Command History

Version 9.3(0.0)	Introduced on the M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module.

Usage Information The text description is displayed in `show fcoe-map` command output.

Related Commands

fcoe-map — creates an FCoE map which contains the parameters used in the communication between servers and a SAN fabric.

show fcoe-map— displays the Fibre Channel and FCoE configuration parameters in FCoE maps.

fabric

Apply an FCoE map on a fabric-facing Fibre Channel (FC) port.

M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module

Syntax `fabric map-name`

Parameters

map-name	Maximum: 32 alphanumeric characters.

Defaults None

Command Modes INTERFACE FIBRE_CHANNEL

Command History

Version 9.3(0.0)	Introduced on the M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module.

Usage Information An FCoE map is a template used to map FCoE and FC parameters in a converged fabric. An FCoE map is used to virtualize upstream FC ports on an M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module NPIV proxy gateway so that they appear to downstream server CNA ports as FCoE forwarder (FCF) ports on an FCoE network. When applied to FC and Ethernet ports on an NPIV proxy gateway, an FCoE map allows the switch to operate as an FCoE-FC bridge between an FC SAN and an FCoE network by providing FCoE-enabled servers and switches with the necessary parameters to log in to a SAN fabric. Use the `fcoe-map` command to create an FCoE map.

On an M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module NPIV proxy gateway, you cannot apply an FCoE map on fabric-facing FC ports and server-facing Ethernet ports.

After you apply an FCoE map on an FC interface, when the port is enabled (`no shutdown`), the NPIV proxy gateway starts sending FIP multicast advertisements on behalf of the FC port to downstream servers in order to advertise the availability of a new FCF port on the FCoE VLAN.

To remove an FCoE map from an FC interface, enter the `no fabric` *`map-name`* command in Interface configuration mode.

Related Commands	fcoe-map — creates an FCoE map which contains the parameters used in the communication between servers and a SAN fabric. show fcoe-map— displays the Fibre Channel and FCoE configuration parameters in FCoE maps.

fabric-id vlan

In an FCoE map, configure the association between the dedicated VLAN used to carry FCoE traffic between servers and a SAN, and the fabric where the desired storage arrays are installed.

M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module

Syntax `fabric-id` *`fabric-num`* `vlan` *`vlan-id`*

Parameters

fabric-id *fabric-num*	Enter a fabric ID number that is the same as the ID number of the dedicated VLAN used to carry FCoE storage traffic to the fabric specified in the FCoE map. You can enter a fabric ID in the range 1–4094.
vlan*vlan-id*	Enter the ID number of the dedicated VLAN used to carry FCoE storage traffic between servers and a SAN fabric and specified with the `vlan` command in the FCoE map.

Defaults	None
Command Modes	FCOE MAP
Command History	

Version 9.3(0.0)	Introduced on the M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module.

Usage Information

In the `fabric-id vlan` command, the fabric and VLAN ID numbers must be the same.

In each FCoE map, the fabric ID, FC-MAP value, and FCoE VLAN parameters must be unique.

To remove a fabric-VLAN association from an FCoE map, enter the `no fabric-id vlan` command.

You must first create a VLAN and then specify the configured VLAN ID in the `fabric-id vlan` command. Otherwise, the following error message is displayed.

```
 FTOS(conf-fcoe-f)#fabric-id 10 vlan 10 % Error: Vlan 10 does
not exist
```

Related Commands

fcoe-map — creates an FCoE map which contains the parameters used in the communication between servers and a SAN fabric.

show fcoe-map— displays the Fibre Channel and FCoE configuration parameters in FCoE maps.

fcf-priority

In an FCoE map, configure the priority used by a server CNA to select an upstream FCoE forwarder (FCF).

M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module

Syntax `fcf—priority priority`

Parameters

priority	Enter the priority assigned to the M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module NPIV proxy gateway, which appears to a downstream server CNA as an FCF. The range of FCF priority values is from 1 to 255.

Defaults 128

Command Modes FCOE MAP

Command History

Version 9.3(0.0)	Introduced on the M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module.

Usage Information

The FCF priority you assign to an M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module is used by server CNAs to select an upstream FCF to use for a fabric login (FLOGI).

To remove a configured FCF priority from an FCoE map, enter the `no fcf-priority` command.

Related Commands	fcoe-map — creates an FCoE map which contains the parameters used in the communication between servers and a SAN fabric. show fcoe-map— displays the Fibre Channel and FCoE configuration parameters in FCoE maps.

fc-map

In an FCoE map, configure the FCoE mapped address prefix (FC-MAP) value which is used to identify FCoE traffic transmitted on the FCoE VLAN for the specified fabric.

M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module

Syntax `fc—map fc-map-value`

Parameters

fc-map-value	Enter the unique MAC address prefix used by a SAN fabric. The range of FC-MAP values is from 0EFC00 to 0EFCFF.

Defaults None

Command Modes FCOE MAP

Command History

Version 9.3(0.0)	Introduced on the M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module.

Usage Information

The FC-MAP value you enter must match the FC-MAP value used by an FC switch or FCoE forwarder (FCF) in the fabric. An FCF switch accepts only FCoE traffic that uses the correct FC-MAP value.

The FC-MAP value is used to generate the fabric-provided MAC address (FP-MAC). The FPMA is used by servers to transmit FCoE traffic to the fabric. An FC-MAP can be associated with only one FCoE VLAN and vice versa.

In an FCoE map, the FC-MAP value, fabric ID, and FCoE VLAN parameters must be unique.

To remove a configured FC-MAP value from an FCoE map, enter the `no fc-map` command.

Related Commands

fcoe-map — creates an FCoE map which contains the parameters used in the communication between servers and a SAN fabric.

show fcoe-map— displays the Fibre Channel and FCoE configuration parameters in FCoE maps.

fcoe priority-bits

Configure the FCoE priority advertised for the FCoE protocol in application priority TLVs.

Syntax	`fcoe priority-bits` *`priority-bitmap`* To remove the configured FCoE priority, use the `no fcoe priority-bits` command.
Parameters	*priority-bitmap* — Enter the priority-bitmap range. The range is from 1 to FF.
Defaults	0x8
Command Modes	PROTOCOL LLDP
Command History	**Version 9.3.0.0** — Introduced on the FC Flex IO module installed in the M I/O Aggregator and MXL 10/40GbE Switch
Usage Information	This command is available at the global level only.

fcoe-map

Create an FCoE map which contains the parameters used to configure the links between server CNAs and a SAN fabric. Apply the FCoE map on a server-facing Ethernet port.

M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module

Syntax	`fcoe-map` *`map-name`*
Parameters	*map-name* — Maximum: 32 alphanumeric characters.
Defaults	None on the MXL 10/40GbE Switch with FC Flex IO modules On the I/O Aggregator with FC Flex IO modules, the following parameters are applied on all the FC Flex IO module interfaces: • Description: SAN_FABRIC • Fabric-id: 1002 • Fcoe-vlan: 1002 • Fc-map: 0x0efc00 • Fcf-priority: 128 • Fka-adv-period: 8000mSec • Keepalive: enable • Vlan priority: 3

Command Modes	CONFIGURATION INTERFACE
Command History	

Version 9.3(0.0)	Introduced on the M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module.

Usage Information

An FCoE map is a template used to map FCoE and FC parameters in a converged fabric. An FCoE map is used to virtualize upstream FC ports on an M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module NPIV proxy gateway so that they appear to downstream server CNA ports as FCoE forwarder (FCF) ports on an FCoE network. When applied to FC and Ethernet ports on an NPIV proxy gateway, an FCoE map allows the switch to operate as an FCoE-FC bridge between an FC SAN and an FCoE network by providing FCoE-enabled servers and switches with the necessary parameters to log in to a SAN fabric.

On an M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module NPIV proxy gateway, you cannot apply an FCoE map is applied on fabric-facing FC ports and server-facing 10–Gigabit Ethernet ports.

An FCoE map consists of the following parameters: the dedicated FCoE VLAN used for storage traffic, the destination SAN fabric (FC-MAP value), FCF priority used by a server, and the FIP keepalive (FKA) advertisement timeout.

In each FCoE map, the fabric ID, FC-MAP value, and FCoE VLAN parameters must be unique. Use one FCoE map to access one SAN fabric. You cannot use the same FCoE map to access different fabrics.

To remove an FCoE map from an Ethernet interface, enter the `no fcoe-map` *`map-name`* command in Interface configuration mode.

Related Commands

show fcoe-map— displays the Fibre Channel and FCoE configuration parameters in FCoE maps.

fka-adv-period

In an FCoE map, configure the time interval used to transmit FIP keepalive (FKA) advertisements.

M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module

Syntax `fka-adv-period` *`seconds`*

Parameters

seconds	Enter the time period (in seconds) used to send FIP keepalive messages to peer devices. The range is from 8 to 90 seconds.

Defaults 8 seconds

Command Modes	FCOE MAP
Command History	**Version 9.3(0.0)** Introduced on the M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module.
Usage Information	To delete the FIP keepalive time period from an FCoE map, enter the `no fka-adv-erpiod` command.
Related Commands	fcoe-map — creates an FCoE map which contains the parameters used in the communication between servers and a SAN fabric. show fcoe-map— displays the Fibre Channel and FCoE configuration parameters in FCoE maps.

interface vlan (NPIV proxy gateway)

Create a dedicated VLAN to be used to send and receive Fibre Channel traffic over FCoE links between servers and a fabric over an M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module NPIV proxy gateway.

M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module

Syntax	`interface vlan vlan-id`	
Parameters	*vlan-id*	Enter a number as the VLAN Identifier. The range is 1 to 4094.
Defaults	Not configured.	
Command Modes	CONFIGURATION	
Command History	**Version 9.3.0.0**	Introduced on the M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module configured as an NPIV proxy gateway.

Usage Information

FCoE storage traffic received from servers on an M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module NPIV proxy gateway is de-capsulated into Fibre Channel packets and forwarded over FC links to SAN switches in a specified fabric. You must configure a separate FCoE VLAN for each fabric to which FCoE traffic is forwarded. Any non-FCoE traffic sent on a dedicated FCoE VLAN will be dropped.

You configure the association between a dedicated VLAN, which carries FCoE traffic from server CNAs over the NPIV proxy gateway to a SAN fabric in which destination storage arrays are installed, in an FCoE map by using the `fabric id vlan` command.

When you apply an FCoE map to a server-facing Ethernet port, the port is automatically configured as a tagged member of the FCoE VLAN.

For more information about VLANs and the commands to configure them, refer to the Virtual LAN (VLAN) Commands section of the Layer 2 chapter.

Example (Single Range)

```
FTOS(conf)#interface vlan 10
FTOS(conf-if-vl-3)#
```

Related Commands

fcoe-map — creates an FCoE map which contains the parameters used in the communication between servers and a SAN fabric.

show fcoe-map— displays the Fibre Channel and FCoE configuration parameters in FCoE maps.

keepalive

In an FCoE map, enable the monitoring of FIP keepalive messages (if it is disabled).

M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module

Syntax `keepalive`

Parameters None

Defaults FIP keepalive monitoring is enabled on Ethernet and Fibre Channel interfaces.

Command Modes FCOE MAP

Command History

Version 9.3(0.0)	Introduced on the M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module.

Usage Information

FIP keepalive (FKA) messaging is used to detect if other FCoE devices are reachable.

To remove FIP keepalive monitoring from an FCoE map, enter the `no keepalive` command.

Related Commands

fcoe-map — creates an FCoE map which contains the parameters used in the communication between servers and a SAN fabric.

show fcoe-map— displays the Fibre Channel and FCoE configuration parameters in FCoE maps.

priority-group bandwidth pfc

Configure the ETS bandwidth allocation and PFC mode used to manage port traffic in an 802.1p priority group.

M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module

Syntax

```
priority-group group-num {bandwidth percentage| strict-
priority} pfc {on | off}
```

Parameters

priority-group *group-num*	Enter the keyword `priority-group` followed by the number of an 802.1p priority group. Use the `priority-pgid` command to create the priority groups in a DCB map.
bandwidth *percentage*	Enter the keyword `bandwidth` followed by a bandwidth percentage allocated to the priority group. The range of valid values is 1 to 100. The sum of all allocated bandwidth percentages in priority groups in a DCB map must be 100%.
strict-priority	Configure the priority-group traffic to be handled with strict priority scheduling. Strict-priority traffic is serviced first, before bandwidth allocated to other priority groups is made available.
pfc {on | off}	Configure whether priority-based flow control is enabled (on) or disabled (off) for port traffic in the priority group.

Defaults None

Command Modes DCB MAP

Command History

Version 9.3(0.0)	Introduced on the M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module.

Usage Information

Use the `dcb-map` command to configure priority groups with PFC and/or ETS settings and apply them to Ethernet interfaces.

Use the `priority-pgid` command to map 802.1p priorities to a priority group. You can assign each 802.1p priority to only one priority group. A priority group consists of 802.1p priority values that are grouped together for similar bandwidth allocation and scheduling, and that share latency and loss requirements. All 802.1p priorities mapped to the same queue must be in the same priority group.

Repeat the `priority-group bandwidth pfc` command to configure PFC and ETS traffic handling for each priority group in a DCB map.

You can enable PFC on a maximum of two priority queues.

If you configure more than one priority group as strict priority, the higher numbered priority queue is given preference when scheduling data traffic.

If a priority group does not use its allocated bandwidth, the unused bandwidth is made available to other priority groups.

To remove a priority-group configuration in a DCB map, enter the `no priority-group bandwidth pfc` command.

By default, equal bandwidth is assigned to each dot1p priority in a priority group. Use the `bandwidth` parameter to configure the bandwidth percentage assigned to a priority group. The sum of the bandwidth allocated to all priority groups in a DCB map must be 100% of the bandwidth on the link. You must allocate at least 1% of the total port bandwidth to each priority group.

Related Commands

dcb-map – creates a DCB map to configure PFC and ETS parameters and applies the PFC and ETS settings on Ethernet ports.

priority-pgid – configures the 802.1p priority traffic in a priority group for a DCB map.

show fcoe-map

Display the Fibre Channel and FCoE configuration parameters in FCoE maps.

M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module

Syntax `show fcoe-map [brief | map-name]`

Parameters

brief	Displays an overview of currently configured FCoE maps.
map-name	Displays the FC and FCoE configuration parameters in a specified FCoE map. The FCoE map is applied on Ethernet (FCoE) and FC ports to transmit FC storage traffic to a specified fabric.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.3(0.0)	Introduced on the M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module.

Usage Information

Use the `show fcoe-map` command to display the FC and FCoE parameters used to configure server-facing Ethernet (FCoE) and fabric-facing FC ports in all FCoE maps on an M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module NPIV proxy gateway.

In each FCoE map, the values for the fabric ID and FC-MAP that identify the SAN fabric to which FC storage traffic is sent, and the FCoE VLAN to be used must be unique.

An FCoE map is used to identify the SAN fabric to which FCoE storage traffic is sent and to virtualize M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module FC ports so that they appear to downstream server CNA ports as FCoE Forwarder (FCF) ports on an FCoE network.

The following table describes the `show fcoe-map brief` output shown in the example below.

Field	Description
Fabric-Name	Name of a SAN fabric.
Fabric ID	The ID number of the SAN fabric to which FC traffic is forwarded.
VLAN ID	The dedicated FCoE VLAN used to transport FCoE storage traffic between servers and a fabric over the NPIV proxy gateway. The configured VLAN ID must be the same as the fabric ID.
FC-MAP	FCoE MAC address-prefix value - The unique 24-bit MAC address prefix that identifies a fabric.
FCF Priority	The priority used by a server to select an upstream FCoE forwarder.
Config-State	Indicates whether the configured FCoE and FC parameters in the FCoE map are valid: Active (all mandatory FCoE and FC parameters are correctly configured) or Incomplete (either the FC-MAP value, fabric ID, or VLAN ID are not correctly configured).
Oper-State	Operational status of link to the fabric: Up (link is up and transmitting FC traffic), Down (link is down and not transmitting FC traffic), Link-wait (link is up and waiting for FLOGI to complete on peer FC port), or Removed (port has been shut down).

The following table describes the `show fcoe-map` *`map-name`* output shown in the example below.

Field	Description
Fabric-Name	Name of a SAN fabric.
Fabric ID	The ID number of the SAN fabric to which FC traffic is forwarded.
VLAN ID	The dedicated FCoE VLAN used to transport FCoE storage traffic between servers and a fabric over the NPIV proxy gateway. The configured VLAN ID must be the same as the fabric ID.
VLAN priority	FCoE traffic uses VLAN priority 3. (This setting is not user-configurable.)

Field	Description
FC-MAP	FCoE MAC address-prefix value - The unique 24-bit MAC address prefix that identifies a fabric.
FKA-ADV-period	Time interval (in seconds) used to transmit FIP keepalive advertisements.
FCF Priority	The priority used by a server to select an upstream FCoE forwarder.
Config-State	Indicates whether the configured FCoE and FC parameters in the FCoE map are valid: Active (all mandatory FCoE and FC parameters are correctly configured) or Incomplete (either the FC-MAP value, fabric ID, or VLAN ID are not correctly configured).
Oper-State	Operational status of link to the fabric: Up (link is up and transmitting FC traffic), Down (link is down and not transmitting FC traffic), Link-wait (link is up and waiting for FLOGI to complete on peer FC port), or Removed (port has been shut down).
Members	M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module Ethernet and FC ports that are members of the dedicated FCoE VLAN that carries storage traffic to the specified fabric.

Example

```
FTOS#show fcoe-map brief
Fabric-Name  Fabric-Id  Vlan-Id  FC-MAP  FCF-Priority Config-
State Oper-State
 test        16          16      0efc02  128
ACTIVE        UP
 cnatest     1003           1003    0efc03  128
ACTIVE        UP
 sitest      1004        1004    0efc04  128
ACTIVE        DOWN


FTOS#show fcoe-map si

Fabric Name        si
Fabric Id          1004
Vlan Id            1004
Vlan priority      3
FC-MAP             0efc04
FKA-ADV-Period     8
Fcf Priority       128
Config-State       ACTIVE
Oper-State         DOWN
Members
```

Related Commands

fcoe-map — creates an FCoE map which contains the parameters used in the communication between servers and a SAN fabric.

show npiv devices

Display the FCoE and FC devices currently logged in to an M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module NPIV proxy gateway.

M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module

Syntax

```
show npiv devices [brief]
```

Parameters

brief	Displays an overview of current server CNA-fabric connections over an M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module NPIV proxy gateway.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.3(0.0)	Introduced on the M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module.

Usage Information

Use the `show npiv devices` command to display information on the server CNA, server-facing Ethernet and fabric-facing FC ports, and the SAN fabric in each server-fabric connection over an M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module NPIV proxy gateway.

The following table describes the `show npiv devices brief` output shown in the example below.

Field	Description
ENode-Intf	M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module Ethernet interface (*slot/port*) to which a server CNA is connected.
ENode-WWPN	Worldwide port name (WWPN) of a server CNA port.
FCoE-Vlan	VLAN ID of the dedicated VLAN used to transmit FCoE traffic to and from the fabric.
Fabric-Intf	Fabric-facing Fibre Channel port (*slot/port*) on which FC traffic is transmitted to the specified fabric.
Fabric-Map	Name of the FCoE map containing the FCoE/FC configuration parameters for the server CNA-fabric connection.
LoginMethod	Method used by the server CNA to log in to the fabric; for example: FLOGI - ENode logged in using a fabric login (FLOGI).

Field	Description
	FDISC - ENode logged in using a fabric discovery (FDISC).
Status	Operational status of the link between a server CNA port and a SAN fabric: Logged In - Server has logged in to the fabric and is able to transmit FCoE traffic.

Example

```
Dell# show npiv devices brief

Total NPIV Devices = 2
---------------------------------------------------------------
----------------------------

ENode-Intf  ENode-WWPN           FCoE-Vlan  Fabric-Intf
Fabric-Map   LoginMethod  Status
---------------------------------------------------------------
---------------------------

Te 0/12     20:01:00:10:18:f1:94:20   1003      Fc 0/5
fid_1003     FLOGI       LOGGED_IN
Te 0/13     10:00:00:00:c9:d9:9c:cb   1003      Fc 0/0
fid_1003     FDISC       LOGGED_IN
```

Usage Information

The following table describes the `show npiv devices` output shown in the example below.

Field	Description
ENode [*number*]	A server CNA that has successfully logged in to a fabric over an M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module Ethernet port in ENode mode.
Enode MAC	MAC address of a server CNA port.
Enode Intf	Port number of a server-facing Ethernet port operating in ENode mode.
FCF MAC	Fibre Channel forwarder MAC: MAC address of M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module FCF interface.
Fabric Intf	Fabric-facing Fibre Channel port (*slot/port*) on which FCoE traffic is transmitted to the specified fabric.
FCoE VLAN	ID of the dedicated VLAN used to transmit FCoE traffic from a server CNA to a fabric and configured on both the server-facing M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module port and server CNA port.
Fabric Map	Name of the FCoE map containing the FCoE/FC configuration parameters for the server CNA-fabric connection.
Enode WWPN	Worldwide port name of the server CNA port.
Enode WWNN	Worldwide node name of the server CNA.

Field	Description
FCoE MAC	Fabric-provided MAC address (FPMA). The FPMA consists of the FC-MAP value in the FCoE map and the FC-ID provided by the fabric after a successful FLOGI. In the FPMA, the most significant bytes are the FC-MAP; the least significant bytes are the FC-ID.
FC-ID	FC port ID provided by the fabric.
LoginMethod	Method used by the server CNA to log in to the fabric; for example, FLOGI or FDISC.
Secs	Number of seconds that the fabric connection is up.
State	Status of the fabric connection: logged in.

Example

```
ENode[0]:
ENode MAC     :     00:10:18:f1:94:21
ENode Intf    :     Te 0/12
FCF MAC       :     5c:f9:dd:ef:10:c8
Fabric Intf   :     Fc 0/5
FCoE Vlan     :     1003
Fabric Map    :     fid_1003
ENode WWPN    :     20:01:00:10:18:f1:94:20
ENode WWNN    :     20:00:00:10:18:f1:94:21
FCoE MAC      :     0e:fc:03:01:02:01
FC-ID         :     01:02:01
LoginMethod   :     FLOGI
Secs          :     5593
Status        :     LOGGED_IN

ENode[1]:
ENode MAC     :     00:10:18:f1:94:22
ENode Intf    :     Te 0/13
FCF MAC       :     5c:f9:dd:ef:10:c9
Fabric Intf   :     Fc 0/0
FCoE Vlan     :     1003
Fabric Map    :     fid_1003
ENode WWPN    :     10:00:00:00:c9:d9:9c:cb
ENode WWNN    :     10:00:00:00:c9:d9:9c:cd
FCoE MAC      :     0e:fc:03:01:02:02
FC-ID         :     01:02:01
LoginMethod   :     FDISC
Secs          :     5593
Status        :     LOGGED_IN
```

Related Commands

dcb-map— creates a DCB map to configure DCB parameters on Ethernet ports that support converged Ethernet traffic.

fcoe-map — creates an FCoE map which contains the parameters used in the communication between servers and a SAN fabric.

64

PMUX Mode of the MXL 10/40GbE Switch I/O Module

This chapter describes the various CLI commands applicable in PMUX mode.

Data Center Bridging (DCB)

Data center bridging (DCB) refers to a set of IEEE Ethernet enhancements that provide data centers with a single, robust, converged network to support multiple traffic types, including local area network (LAN), server, and storage traffic.

The Dell Networking Operating System (OS) commands for data center bridging features include 802.1Qbb priority-based flow control (PFC), 802.1Qaz enhanced transmission selection (ETS), and the data center bridging exchange (DCBX) protocol.

advertise dcbx-appln-tlv

On a DCBX port with a manual role, configure the application priority TLVs advertised on the interface to DCBX peers.

Syntax

```
advertise dcbx-appln-tlv {fcoe | iscsi}
```

To remove the application priority TLVs, use the `no advertise dcbx-appln-tlv {fcoe | iscsi}` command.

Parameters

{fcoe | iscsi}	Enter the application priority TLVs, where: • `fcoe`: enables the advertisement of FCoE in application priority TLVs. • `iscsi`: enables the advertisement of iSCSI in application priority TLVs.

Defaults

Application priority TLVs are enabled to advertise FCoE and iSCSI.

Command Modes

PROTOCOL LLDP

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information	To disable TLV transmission, use the `no` form of the command; for example, `no advertise dcbx-appln-tlv iscsi`.

advertise dcbx-tlv

On a DCBX port with a manual role, configure the PFC and ETS TLVs advertised to DCBX peers.

Syntax

`advertise dcbx-tlv {ets-conf | ets-reco | pfc} [ets-conf | ets-reco | pfc] [ets-conf | ets-reco | pfc]`

To remove the advertised ETS TLVs, use the `no advertise dcbx-tlv` command.

Parameters

{ets-conf | ets-reco | pfc}	Enter the PFC and ETS TLVs advertised, where: • `ets-conf:` enables the advertisement of ETS configuration TLVs. • `ets-reco:` enables the advertisement of ETS recommend TLVs. • `pfc:` enables the advertisement of PFC TLVs.

Defaults

All PFC and ETS TLVs are advertised.

Command Modes

PROTOCOL LLDP

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

You can configure the transmission of more than one TLV type at a time; for example: `advertise dcbx-tlv ets-conf ets-reco`.

You can enable ETS recommend TLVs (`ets-reco`) only if you enable ETS configuration TLVs (`ets-conf`). To disable TLV transmission, use the `no` form of the command; for example, `no advertise dcbx-tlv pfc ets-reco`.

DCBX requires that you enable LLDP to advertise DCBX TLVs to peers.

Configure DCBX operation at the INTERFACE level on a switch or globally on the switch. To verify the DCBX configuration on a port, use the `show interface dcbx detail` command.

bandwidth-percentage

Configure the bandwidth percentage allocated to priority traffic in port queues.

Syntax

`bandwidth-percentage` *`percentage`*

To remove the configured bandwidth percentage, use the `no bandwidth-percentage` command.

Parameters		
	percentage	(Optional) Enter the bandwidth percentage. The percentage range is from 1 to 100% in units of 1%.

Defaults

none

Command Modes

QOS-POLICY-OUT-ETS

Command History		
	Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

By default, equal bandwidth is assigned to each port queue and each dot1p priority in a priority group. To configure bandwidth amounts in associated dot1p queues, use the `bandwidth-percentage` command. When specified bandwidth is assigned to some port queues and not to others, the remaining bandwidth (100% minus assigned bandwidth amount) is equally distributed to unassigned nonstrict priority queues in the priority group. The sum of the allocated bandwidth to all queues in a priority group must be 100% of the bandwidth on the link.

ETS-assigned bandwidth allocation applies only to data queues, not to control queues.

The configuration of bandwidth allocation and strict-queue scheduling is not supported at the same time for a priority group. If you configure both, the configured bandwidth allocation is ignored for priority-group traffic when you apply the output policy on an interface.

By default, equal bandwidth is assigned to each priority group in the ETS output policy applied to an egress port if you did not configure bandwidth allocation. The sum of configured bandwidth allocation to dot1p priority traffic in all ETS priority groups must be 100%. Allocate at least 1% of the total bandwidth to each priority group and queue. If bandwidth is assigned to some priority groups but not to others, the remaining bandwidth (100% minus assigned bandwidth amount) is equally distributed to nonstrict-priority groups which have no configured scheduler.

Related Commands

- qos-policy-output ets — creates a QoS output policy.
- scheduler — schedules priority traffic in port queues.

dcb-enable

Enable data center bridging.

Syntax

```
dcb enable
```

To disable DCB, use the `no dcb enable` command.

Defaults	none
Command Modes	CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

DCB is not supported if you enable `link-level flow control` on one or more interfaces.

dcb-input

To apply pause or flow control for specified priorities using a configure delay time, create a DCB input policy.

Syntax

`dcb-input` *`policy-name`*

To delete the DCB input policy, use the `no dcb-input` command.

Parameters

policy-name	Maximum: 32 alphanumeric characters.

Defaults	none
Command Modes	CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

As soon as you apply a DCB policy with PFC enabled on an interface, DCBx starts exchanging information with PFC-enabled peers. The IEEE802.1Qbb, CEE, and CIN versions of PFC TLV are supported. DCBx also validates PFC configurations received in TLVs from peer devices.

By applying a DCB input policy with PFC enabled, you enable PFC operation on ingress port traffic. To achieve complete lossless handling of traffic, also enable PFC on all DCB egress ports or configure the dot1p priority-queue assignment of PFC priorities to lossless queues (refer to `pfc no-drop queues`).

To remove a DCB input policy, including the PFC configuration it contains, enter the `no dcb-input` *`policy-name`* command in Interface Configuration mode.

NOTE: Please note that Dell Networking does not recommended to use this command as it has been deprecated in the current 9.4(0.0) release. A warning message appears when you try to run this command indicating that you have to use the `dcb-map` commands in the future.

Related Commands	dcb-policy input — applies the input policy with the PFC configuration.

dcb-output

To associate an ETS configuration with priority traffic, create a DCB output policy.

Syntax

`dcb-output policy-name`

To remove the ETS output policy globally, use the `no dcb output policy-name` command.

Parameters

policy-name	Enter the DCB output policy name. The maximum is 32 alphanumeric characters.

Defaults none

Command Modes CONFIGURATION

Command History

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To associate a priority group with an ETS output policy with scheduling and bandwidth configuration, create a DCB output policy. You can apply a DCB output policy on multiple egress ports. When you apply an ETS output policy on an interface, ETS-configured scheduling and bandwidth allocation take precedence over any configured settings in QoS output policies.

The ETS configuration associated with 802.1 priority traffic in a DCB output policy is used in DCBX negotiation with ETS peers.

NOTE: Please note that Dell Networking does not recommended to use this command as it has been deprecated in the current 9.4(0.0) release. A warning message appears when you try to run this command indicating that you have to use the `dcb-map` commands in the future.

Related Commands dcb-policy output — applies the output policy.

dcb-policy input

Apply the input policy with the PFC configuration to an ingress interface.

Syntax

`dcb-policy input policy-name`

To delete the input policy, use the `no dcb-policy input` command.

Parameters

policy-name	Enter the input policy name with the PFC configuration to an ingress interface.

Defaults

none

Command Modes

INTERFACE

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

If you apply an input policy with PFC disabled (`no pfc mode on`):

- You can enable link-level flow control on the interface. To delete the input policy, first disable link-level flow control. PFC is then automatically enabled on the interface because an interface is by default PFC-enabled.
- PFC still allows you to configure lossless queues on a port to ensure no-drop handling of lossless traffic.

When you apply an input policy to an interface, an error message is displayed if:

- The PFC dot1p priorities result in more than two lossless port queues globally on the switch.
- You already enabled link-level flow control. PFC and link-level flow control cannot be enabled at the same time on an interface.

In a switch stack, configure all stacked ports with the same PFC configuration.

A DCB input policy for PFC applied to an interface may become invalid if you reconfigure the dot1p-queue mapping. This situation occurs when the new dot1p-queue assignment exceeds the maximum number (2) of lossless queues supported globally on the switch. In this case, all PFC configurations received from PFC-enabled peers are removed and resynchronized with the peer devices.

Traffic may be interrupted when you reconfigure PFC no-drop priorities in an input policy or reapply the policy to an interface.

NOTE: Please note that Dell Networking does not recommended to use this command as it has been deprecated in the current 9.4.(0.0) release. A warning message appears when you try to run this command indicating that you have to use the `dcb-map` commands in the future.

Related Commands

dcb-input — creates a DCB input policy.

dcb-policy input stack-unit stack-ports all

Apply the specified DCB input policy on all ports of the switch stack or a single stacked switch.

Syntax

```
dcb-policy input stack-unit {all | stack-unit-id} stack-ports
all dcb-input-policy-name
```

To remove all DCB input policies applied to the stacked ports and rest the PFC to its default settings, use the `no dcb-policy input stack-unit all` command.

To remove only the DCB input policies applied to the specified switch, use the `no dcb-policy input stack-unit` command.

Parameters

stack-unit-id	Enter the stack unit identification.
dcb-input-policy-name	Enter the policy name for the DCB input policy.

Defaults: none

Command Modes: CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The `dcb-policy input stack-unit all` command overwrites any previous `dcb-policy input stack-unit stack-unit-id` configurations. Similarly, a `dcb-policy input stack-unit stack-unit-id` command overwrites any previous `dcb-policy input stack-unit all` configuration.

NOTE: Please note that Dell Networking does not recommended to use this command as it has been deprecated in the current 9.4.(0.0) release. A warning message appears when you try to run this command indicating that you have to use the `dcb-map` commands in the future.

Related Commands

dcb-policy output stack-unit stack-ports all — applies the specified DCB output policy.

dcb-policy output

Apply the output policy with the ETS configuration to an egress interface.

Syntax

`dcb-policy output` *`policy-name`*

To delete the output policy, use the `no dcb-policy output` command.

Parameters

policy-name	Enter the output policy name.

Defaults: none

Command Modes: INTERFACE

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information	When you apply an ETS output policy to on interface, ETS-configured scheduling and bandwidth allocation take precedence over any configured settings in QoS output policies. To remove an ETS output policy from an interface, use the `no dcb-policy output policy-name` command. ETS is enabled by default with the default ETS configuration applied (all dot1p priorities in the same group with equal bandwidth allocation). NOTE: Please note that Dell Networking does not recommended to use this command as it has been deprecated in the current 9.4(0.0) release. A warning message appears when you try to run this command indicating that you have to use the `dcb-map` commands in the future.
Related Commands	dcb-output — creates a DCB output policy.

dcb-policy output stack-unit stack-ports all

Apply the specified DCB output policy on all ports of the switch stack or a single stacked switch.

Syntax	`dcb-policy output stack-unit {all | stack-unit-id} stack-ports all dcb-output-policy-name` To remove all DCB output policies applied to the stacked ports, use the `no dcb-policy output stack-unit all` command. To remove only the DCB output policies applied to the specified switch, use the `no dcb-policy output stack-unit` command.
Parameters	*stack-unit-id* — Enter the stack unit identification. *dcb-output-policy-name* — Enter the policy name for the DCB output policy.
Defaults	none
Command Modes	CONFIGURATION
Command History	Version 9.2(0.0) — Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only. Version 8.3.16.1 — Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	The `dcb-policy output stack-unit all` command overwrites any previous `dcb-policy output stack-unit stack-unit-id` configurations. Similarly, a `dcb-policy output stack-unit stack-unit-id` command overwrites any previous `dcb-policy output stack-unit all` configuration.

You can apply a DCB output policy with ETS configuration to all stacked ports in a switch stack or an individual stacked switch. You can apply different DCB output policies to different stack units.

NOTE: Please note that Dell Networking does not recommended to use this command as it has been deprecated in the current 9.4.(0.0) release. A warning message appears when you try to run this command indicating that you have to use the `dcb-map` commands in the future.

Related Commands

dcb-policy input stack-unit stack-ports all — applies the specified DCB input policy.

dcb stack-unit all pfc-buffering pfc-port-count pfc-queues

Configure the PFC buffer for all switches in the stack.

Syntax

```
dcb stack-unit all pfc-buffering pfc-port-count {1-56} pfc-queues {1-2}
```

To remove the configuration for the PFC buffer on all switches in the stack, use the `no dcb stack-unit all pfc-buffering pfc-port-count pfc-queues` command.

Parameters

pfc-port-count *{1-56}*	Enter the pfc-port count. The range is 1 to 56.
pfc-queues *{1-2}*	Enter the pfc-queue number. The range is 1 to 2.

Defaults

The PFC buffer is enabled on all ports on the stack unit.

Command Modes

CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

If you configure PFC on a 40GbE port, count the 40GbE port as four PFC-enabled ports in the pfc-port number you enter in the command syntax.

To achieve lossless PFC operation, the PFC port count and queue number used for the reserved buffer size that is created must be greater than or equal to the buffer size required for PFC-enabled ports and lossless queues on the switch.

You must reload the stack or a specified stack unit (use the reload command in EXEC Privilege mode) for the PFC buffer configuration to take effect.

Related Commands

dcb stack-unit pfc-buffering pfc-port pfc-queues – configures the PFC buffer for all port pipes in a specified stack unit.

dcb stack-unit pfc-buffering pfc-port-count pfc-queues

Configure the PFC buffer for all port pipes in a specified stack unit by specifying the port-pipe number, number of PFC-enabled ports, and number of configured lossless queues.

Syntax

`dcb stack-unit stack-unit-id [port-set port-set-id] pfc-buffering pfc-ports {1-56} pfc-queues {1-2}`

To remove the configuration for the PFC buffer on all port pipes in a specified stack unit, use the `no dcb stack-unit stack-unit-id [port-set port-set-id] pfc-buffering pfc-ports pfc-queues` command.

Parameters

stack-unit-id	Enter the stack unit identification. The range is from 0 to 5.
port-set	Enter the port-set identification. The only valid port-set ID (port-pipe number) on an MXL Switch is 0.
pfc-ports *{1-56}*	Enter the pfc-ports. The range is from 1 to 56.
pfc-queues *{1-2}*	Enter the pfc-queue number. The range is from 1 to 2.

Command Modes

CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

If you configure PFC on a 40GbE port, count the 40GbE port as four PFC-enabled ports in the pfc-port number you enter in the command syntax.

To achieve lossless PFC operation, the PFC port count and queue number used for the reserved buffer size that is created must be greater than or equal to the buffer size required for PFC-enabled ports and lossless queues on the switch.

You must reload the stack or a specified stack unit (use the `reload` command in EXEC Privilege mode) for the PFC buffer configuration to take effect.

Related Commands

dcb stack-unit pfc-buffering pfc-port pfc-queues — configures the PFC buffer for all switches in the stack.

dcbx port-role

Configure the DCBX port role the interface uses to exchange DCB information.

Syntax

`dcbx port-role {config-source | auto-downstream | auto-upstream | manual}`

To remove DCBX port role, use the `no dcbx port-role {config-source | auto-downstream | auto-upstream | manual}` command.

Parameters

config-source | auto-downstream | auto-upstream | manual	Enter the DCBX port role, where: • `config-source`: configures the port to serve as the configuration source on the switch. • `auto-upstream`: configures the port to receive a peer configuration. The configuration source is elected from auto-upstream ports. • `auto-downstream`: configures the port to accept the internally propagated DCB configuration from a configuration source. • `manual`: configures the port to operate only on administer-configured DCB parameters. The port does not accept a DCB configuration received form a peer or a local configuration source.

Defaults **Manual**

Command Modes INTERFACE PROTOCOL LLDP

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

DCBX requires that you enable LLDP to advertise DCBX TLVs to peers.

Configure DCBX operation at the INTERFACE level on a switch or globally on the switch. To verify the DCBX configuration on a port, use the `show interface dcbx detail` command.

dcbx version

Configure the DCBX version used on the interface.

Syntax `dcbx version {auto | cee | cin | ieee-v2.5}`

To remove the DCBX version, use the `dcbx version {auto | cee | cin | ieee-v2.5}` command.

Parameters

auto | cee | cin | ieee-v2.5	Enter the DCBX version type used on the interface, where: • `auto`: configures the port to operate using the DCBX version received from a peer. • `cee`: configures the port to use CDD (Intel 1.01). • `cin`: configures the port to use Cisco-Intel-Nuova (DCBX 1.0).

- `ieee-v2`: configures the port to use IEEE 802.1az (Draft 2.5).

Defaults	**Auto**
Command Modes	INTERFACE PROTOCOL LLDP
Command History	Version 9.2(0.0) — Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only. Version 8.3.16.1 — Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	DCBX requires that you enable LLDP to advertise DCBX TLVs to peers. Configure DCBX operation at the INTERFACE level on a switch or globally on the switch. To verify the DCBX configuration on a port, use the `show interface dcbx detail` command.

debug dcbx

Enable DCBX debugging.

Syntax

```
debug dcbx {all | auto-detect-timer | config-exchng | fail |
mgmt | resource | sem | tlv}
```

To disable DCBX debugging, use the `no debug dcbx` command.

Parameters

{all | auto-detect-timer | config-exchng | fail | mgmt | resource | sem | tlv}	Enter the type of debugging, where: • `all`: enables all DCBX debugging operations. • `auto-detect-timer`: enables traces for DCBX auto-detect timers. • `config-exchng`: enables traces for DCBX configuration exchanges. • `fail`: enables traces for DCBX failures. • `mgmt`: enables traces for DCBX management frames. • `resource`: enables traces for DCBX system resource frames. • `sem`: enables traces for the DCBX state machine. • `tlv`: enables traces for DCBX TLVs.

Defaults	none
Command Modes	EXEC Privilege
Command History	Version 9.2(0.0) — Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

description

Enter a text description of the DCB policy (PFC input or ETS output).

Syntax

`description text`

To remove the text description, use the `no description` command.

Parameters

text	Enter the description of the output policy. The maximum is 32 characters.

Defaults

none

Command Modes

- DCB INPUT POLICY
- DCB OUTPUT POLICY

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

- dcb-input — creates a DCB PFC input policy.
- dcb-policy input — applies the output policy.
- dcb-output — creates a DCBETS output policy.
- dcb-policy output — applies the output policy.

ets mode on

Enable the ETS configuration so that scheduling and bandwidth allocation configured in an ETS output policy or received in a DCBX TLV from a peer can take effect on an interface.

Syntax

`ets mode on`

To remove the ETS configuration, use the `no ets mode on` command.

Defaults

ETS mode is on.

Command Modes

DCB OUTPUT POLICY

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information	If you disable ETS in an output policy applied to an interface using the `no ets mode on` command, any previously configured QoS settings at the interface or global level takes effect. If you configure QoS settings at the interface or global level and in an output policy map (the `service-policy output` command), the QoS configuration in the output policy takes precedence.

NOTE: Please note that Dell Networking does not recommended to use this command as it has been deprecated in the current 9.4(0.0) release. A warning message appears when you try to run this command indicating that you have to use the `dcb-map` commands in the future.

Related Commands

- dcb-output — creates a DCB output policy.
- dcb-policy output — applies the output policy.

fcoe priority-bits

Configure the FCoE priority advertised for the FCoE protocol in application priority TLVs.

Syntax `fcoe priority-bits` *`priority-bitmap`*

To remove the configured FCoE priority, use the `no fcoe priority-bits` command.

Parameters

priority-bitmap	Enter the priority-bitmap range. The range is from 1 to FF.

Defaults 0x8

Command Modes PROTOCOL LLDP

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information This command is available at the global level only.

iscsi priority-bits

Configure the iSCSI priority advertised for the iSCSI protocol in application priority TLVs.

Syntax `iscsi priority-bits` *`priority-bitmap`*

To remove the configured iSCSI priority, use the `no iscsi priority-bits` command.

Parameters

priority-bitmap	Enter the priority-bitmap range. The range is from 1 to FF.

Defaults	0x10
Command Modes	PROTOCOL LLDP

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information: This command is available at the global level only.

pfc link-delay

Configure the link delay used to pause specified priority traffic.

Syntax

```
pfc link-delay value
```

To remove the link delay, use the `no pfc link-delay` command.

Parameters

value	The range is (in quanta) from 712 to 65535. One quantum is equal to a 512-bit transmission.

Defaults	**45556** quantum
Command Modes	DCB INPUT POLICY

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information: The minimum link delay must be greater than the round-trip transmission time a peer must honor a PFC pause frame multiplied by the number of PFC-enabled ingress ports.

Related Commands: dcb-input — creates a DCB input policy.

pfc mode on

Enable the PFC configuration on the port so that the priorities are included in DCBX negotiation with peer PFC devices.

Syntax

```
pfc mode on
```

To disable the PFC configuration, use the `no pfc mode on` command.

Defaults: PFC mode is on.

Command Modes	DCB INPUT POLICY
Command History	**Version 9.2(0.0)** Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only. **Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	By applying a DCB input policy with PFC enabled, you enable PFC operation on ingress port traffic. To achieve complete lossless handling of traffic, also enable PFC on all DCB egress ports or configure the dot1p priority-queue assignment of PFC priorities to lossless queues (refer to `pfc no-drop queues`). To disable PFC operation on an interface, enter the `no pfc mode on` command in DCB Input Policy Configuration mode. PFC is enabled and disabled as global DCB operation is enabled (`dcb-enable`) or disabled (`no dcb-enable`). You cannot enable PFC and link-level flow control at the same time on an interface.
Related Commands	dcb-input — creates a DCB input policy.

pfc no-drop queues

Configure the port queues that still function as no-drop queues for lossless traffic.

Syntax	`pfc no-drop queues` *`queue-range`* To remove the no-drop port queues, use the `no pfc no-drop queues` command.
Parameters	*queue-range* Enter the queue range. Separate the queue values with a comma; specify a priority range with a dash; for example, `pfc no-drop queues 1,3` or `pfc no-drop queues 2-3`. The range is from 0 to 3.
Defaults	No lossless queues are configured.
Command Modes	INTERFACE
Command History	**Version 9.2(0.0)** Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only. **Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	The maximum number of lossless queues globally supported on the switch is two. • The following lists the dot1p priority-queue assignments.

dot1p Value in the Incoming Frame	Description heading
0	0
1	0
2	0
3	1
4	2
5	3
6	3
7	3

pfc priority

Configure the CoS traffic to be stopped for the specified delay.

Syntax

`pfc priority` *`priority-range`*

To delete the pfc priority configuration, use the `no pfc priority` command.

Parameters

priority-range	Enter the 802.1p values of the frames to be paused. Separate the priority values with a comma; specify a priority range with a dash; for example, pfc priority 1,3,5-7. The range is from 0 to 7.

Defaults

none

Command Modes

DCB INPUT POLICY

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

You can enable any number of 802.1p priorities for PFC. Queues to which PFC priority traffic is mapped are lossless by default. Traffic may be interrupted due to an interface flap (going down and coming up) when you reconfigure the lossless queues for no-drop priorities in a PFC input policy and reapply the policy to an interface.

The maximum number of lossless queues supported on the I/O Aggregator switch is four.

A PFC peer must support the configured priority traffic (as DCBX detects) to apply PFC.

NOTE: Please note that Dell Networking does not recommended to use this command as it has been deprecated in the current 9.4(0.0) release. A warning message appears when you try to run this command indicating that you have to use the `dcb-map` commands in the future.

Related Commands	dcb-input — creates a DCB input policy.

priority-group

To use with an ETS output policy, create an ETS priority group.

Syntax

`priority-group group-name`

To remove the priority group, use the `no priority-group` command.

Parameters

group-name	Enter the name of the ETS priority group. The maximum is 32 characters.

Defaults none

Command Modes CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

A priority group consists of 802.1p priority values that are grouped for similar bandwidth allocation and scheduling, and that share latency and loss requirements. All 802.1p priorities mapped to the same queue must be in the same priority group.

You must configure 802.1p priorities in priority groups associated with an ETS output policy. You can assign each dot1p priority to only one priority group.

The maximum number of priority groups supported in ETS output policies on an interface is equal to the number of data queues (4) on the port. The 802.1p priorities in a priority group can map to multiple queues.

If you configure more than one priority queue as strict priority or more than one priority group as strict priority, the higher numbered priority queue is given preference when scheduling data traffic.

NOTE: Please note that Dell Networking does not recommended to use this command as it has been deprecated in the current 9.4(0.0) release. A warning message appears when you try to run this command indicating that you have to use the `dcb-map` commands in the future.

Related Commands	- priority-list — configures the 802.1p priorities for an ETS output policy. - set-pgid — configures the priority-group.

priority-group qos-policy

Associate the 802.1p priority traffic in a priority group with the ETS configuration in a QoS output policy.

Syntax

`priority-group group-name qos-policy ets-policy-name`

To remove the 802.1p priority group, use the `no priority-group qos-policy` command.

Parameters

group-name	Enter the group name of the 802.1p priority group. The maximum is 32 characters.
ets-policy-name	Enter the ETS policy name.

Defaults

none

Command Modes

DCB OUTPUT POLICY

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The ETS configuration associated with 802.1p priority traffic in a DCB output policy is used in DCBX negotiation with ETS peers.

If you disable ETS in an output policy applied to an interface using the `no ets mode on` command, any previously configured QoS settings at the interface or global level take effect. If you configure QoS settings at the interface or global level and in an output policy map (the `service-policy output` command), the QoS configuration in the output policy takes precedence.

NOTE: Please note that Dell Networking does not recommended to use this command as it has been deprecated in the current 9.4(0.0) release. A warning message appears when you try to run this command indicating that you have to use the `dcb-map` commands in the future.

Related Commands

- dcb-output — creates a DCB output policy.
- dcb-policy output — applies the output policy.

priority-list

Configure the 802.1p priorities for the traffic on which you want to apply an ETS output policy.

Syntax	`priority-list value` To remove the priority list, use the `no priority-list` command.
Parameters	*value*: Enter the priority list value. Separate priority values with a comma; specify a priority range with a dash; for example, priority-list 3,5-7. The range is from 0 to 7.
Defaults	none
Command Modes	PRIORITY-GROUP
Command History	**Version 9.2(0.0)**: Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only. **Version 8.3.16.1**: Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

By default:

- All 802.1p priorities are grouped in priority group 0.
- 100% of the port bandwidth is assigned to priority group 0. The complete bandwidth is equally assigned to each priority class so that each class has 12 to 13%.

NOTE: Please note that Dell Networking does not recommended to use this command as it has been deprecated in the current 9.4(0.0) release. A warning message appears when you try to run this command indicating that you have to use the `dcb-map` commands in the future.

Related Commands

- priority-group qos-policy — associates an ETS priority group with an ETS output policy.
- set-pgid — configures the priority-group.

qos-policy-output ets

To configure the ETS bandwidth allocation and scheduling for priority traffic, create a QoS output policy.

Syntax	`qos-policy-output policy-name ets` To remove the QoS output policy, use the `no qos-policy-output ets` command.
Parameters	*policy-name*: Enter the policy name. The maximum is 32 characters.

Command Modes	CONFIGURATION
Command History	**Version 9.2(0.0)** Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only. **Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

If an error occurs in an ETS output-policy configuration, the configuration is ignored and the scheduler and bandwidth allocation settings are reset to the ETS default values (all priorities are in the same ETS priority group and bandwidth is allocated equally to each priority).

If an error occurs when a port receives a peer's ETS configuration, the port's configuration is reset to the previously configured ETS output policy. If no ETS output policy was previously applied, the port is reset to the default ETS parameters.

Related Commands

- scheduler — schedules the priority traffic in port queues.
- bandwidth-percentage — bandwidth percentage allocated to the priority traffic in port queues.

scheduler

Configure the method used to schedule priority traffic in port queues.

Syntax

`scheduler value`

To remove the configured priority schedule, use the `no scheduler` command.

Parameters

value	Enter schedule priority value. The valid values are: • `strict`: strict-priority traffic is serviced before any other queued traffic. • `werr`: weighted elastic round robin (werr) provides low-latency scheduling for priority traffic on port queues.

Defaults

Weighted elastic round robin (WERR) scheduling is used to queue priority traffic.

Command Modes

POLICY-MAP-OUT-ETS

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

dot1p priority traffic on the switch is scheduled to the current queue mapping. dot1p priorities within the same queue must have the same traffic properties and scheduling method.

ETS-assigned scheduling applies only to data queues, not to control queues.

The configuration of bandwidth allocation and strict-queue scheduling is not supported at the same time for a priority group. If you configure both, the configured bandwidth allocation is ignored for priority-group traffic when you apply the output policy on an interface.

Related Commands

- qos-policy-output ets — configures the ETS bandwidth allocation.
- bandwidth-percentage — bandwidth percentage allocated to priority traffic in port queues.

set-pgid

Configure the priority-group identifier.

Syntax

`set-pgid value`

To remove the priority group, use the `no set-pgid` command.

Parameters

value	Enter the priority group identification. The range is from 0 to 7.

Defaults

none

Command Modes

PRIORITY-GROUP

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

NOTE: Please note that Dell Networking does not recommended to use this command as it has been deprecated in the current 9.4(0.0) release. A warning message appears when you try to run this command indicating that you have to use the `dcb-map` commands in the future.

Related Commands

- priority-group qos-policy — creates an ETS priority group.
- priority-list — configures the 802.1p priorities.

show dcb

Displays the data center bridging status, the number of PFC-enabled ports, and the number of PFC-enabled queues.

Syntax	`show dcb [stack-unit unit-number]`
Parameters	*unit number* — Enter the DCB unit number. The range is from 0 to 5.
Command Modes	EXEC Privilege
Command History	Version 9.2(0.0) — Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only. Version 8.3.16.1 — Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	Specify a stack-unit number on the Master switch in a stack.

Example

```
Dell(conf)#do show  dcb
stack-unit 0 port-set 0
DCB Status         :Enabled
PFC Queue Count    :2
Total Buffer[lossy + lossless] (in KB):7982
PFC Total Buffer (in KB)              :5872
PFC Shared Buffer (in KB)             :832
PFC Available Buffer (in KB)          :4860
Dell (conf)#
```

show interface dcbx detail

Displays the DCBX configuration on an interface.

Syntax	`show interface port-type slot/port dcbx detail`
Parameters	*port-type* — Enter the port type. *slot/port* — Enter the slot/port number.
Command Modes	CONFIGURATION
Command History	Version 9.2(0.0) — Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only. Version 8.3.16.1 — Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	To clear DCBX frame counters, use the `clear dcbx counters interface` *`stack-unit/port`* command.

The following describes the `show interface dcbx detail` command shown in the following example.

Field	Description
Interface	Interface type with chassis slot and port number.
Port-Role	Configured the DCBX port role: auto-upstream, auto-downstream, config-source, or manual.
DCBX Operational Status	Operational status (enabled or disabled) used to elect a configuration source and internally propagate a DCB configuration. The DCBX operational status is the combination of PFC and ETS operational status.
Configuration Source	Specifies whether the port serves as the DCBX configuration source on the switch: true (yes) or false (no).
Local DCBX Compatibility mode	DCBX version accepted in a DCB configuration as compatible. In auto-upstream mode, a port can only receive a DCBX version supported on the remote peer.
Local DCBX Configured mode	DCBX version configured on the port: CEE, CIN, IEEE v2.5, or Auto (port auto-configures to use the DCBX version received from a peer).
Peer Operating version	DCBX version that the peer uses to exchange DCB parameters.
Local DCBX TLVs Transmitted	Transmission status (enabled or disabled) of advertised DCB TLVs (see TLV code at the top of the show command output).
Local DCBX Status: DCBX Operational Version	DCBX version advertised in Control TLVs.
Local DCBX Status: DCBX Max Version Supported	Highest DCBX version supported in Control TLVs.
Local DCBX Status: Sequence Number	Sequence number transmitted in Control TLVs.
Local DCBX Status: Acknowledgment Number	Acknowledgement number transmitted in Control TLVs.
Local DCBX Status: Protocol State	Current operational state of the DCBX protocol: ACK or IN-SYNC.

Field	Description
Peer DCBX Status: DCBX Operational Version	DCBX version advertised in Control TLVs received from the peer device.
Peer DCBX Status: DCBX Max Version Supported	Highest DCBX version supported in Control TLVs received from the peer device.
Peer DCBX Status: Sequence Number	Sequence number transmitted in Control TLVs received from the peer device.
Peer DCBX Status: Acknowledgment Number	Acknowledgement number transmitted in Control TLVs received from the peer device.
Total DCBX Frames transmitted	Number of DCBX frames sent from the local port.
Total DCBX Frames received	Number of DCBX frames received from the remote peer port.
Total DCBX Frame errors	Number of DCBX frames with errors received.
Total DCBX Frames unrecognized	Number of unrecognizable DCBX frames received.

Example

```
Dell(conf)# show interface tengigabitethernet 0/49 dcbx detail
Dell#show interface te 0/49 dcbx detail

E-ETS Configuration TLV enabled
  e-ETS Configuration TLV disabled
R-ETS Recommendation TLV enabled
  r-ETS Recommendation TLV disabled
P-PFC Configuration TLV enabled
  p-PFC Configuration TLV disabled
F-Application priority for FCOE enabled
  f-Application Priority for FCOE disabled
I-Application priority for iSCSI enabled
  i-Application Priority for iSCSI disabled
-----------------------------------------------------------

Interface TenGigabitEthernet 0/49
  Remote Mac Address 00:00:00:00:00:11
   Port Role is Auto-Upstream
  DCBX Operational Status is Enabled
  Is Configuration Source? TRUE

Local DCBX Compatibility mode is CEE
  Local DCBX Configured mode is CEE
  Peer Operating version is CEE
  Local DCBX TLVs Transmitted: ErPfi

Local DCBX Status
-----------------
```

```
  DCBX Operational Version is 0
  DCBX Max Version Supported is 0
  Sequence Number: 2
  Acknowledgment Number: 2
  Protocol State: In-Sync

Peer DCBX Status:
----------------
  DCBX Operational Version is 0
  DCBX Max Version Supported is 255
  Sequence Number: 2
  Acknowledgment Number: 2
  Total DCBX Frames transmitted 27
  Total DCBX Frames received 6
  Total DCBX Frame errors 0
  Total DCBX Frames unrecognized 0
```

show interface ets

Displays the ETS configuration applied to egress traffic on an interface, including priority groups with priorities and bandwidth allocation.

Syntax

`show interface port-type slot/port ets {summary | detail}`

Parameters

port-type slot/port ets	Enter the port-type slot and port ETS information.
{summary | detail}	Enter the keyword `summary` for a summary list of results or enter the keyword `detail` for a full list of results.

Command Modes

CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To clear ETS TLV counters, use the `clear ets counters interface port-type slot/port` command.

The following describes the `show interface summary` command shown in the following example.

Field	Description
Interface	Interface type with stack-unit and port number.
Max Supported TC Group	Maximum number of priority groups supported.
Number of Traffic Classes	Number of 802.1p priorities currently configured.

Field	Description
Admin mode	ETS mode: on or off. When on, the scheduling and bandwidth allocation configured in an ETS output policy or received in a DCBX TLV from a peer can take effect on an interface.
Admin Parameters	ETS configuration on local port, including priority groups, assigned dot1p priorities, and bandwidth allocation.
Remote Parameters	ETS configuration on remote peer port, including admin mode (enabled if a valid TLV was received or disabled), priority groups, assigned dot1p priorities, and bandwidth allocation. If ETS admin mode is enabled on the remote port for DCBX exchange, the Willing bit received in ETS TLVs from the remote peer is included.
Local Parameters	ETS configuration on local port, including admin mode (enabled when a valid TLV is received from a peer), priority groups, assigned dot1p priorities, and bandwidth allocation.
Operational status (local port)	Port state for current operational ETS configuration: • `Init`: Local ETS configuration parameters were exchanged with the peer. • `Recommend`: Remote ETS configuration parameters were received from the peer. • `Internally propagated`: ETS configuration parameters were received from the configuration source.
ETS DCBX Oper status	Operational status of the ETS configuration on the local port: match or mismatch.
State Machine Type	Type of state machine used for DCBX exchanges of ETS parameters: Feature — for legacy DCBX versions; Asymmetric — for an IEEE version.
Conf TLV Tx Status	Status of ETS Configuration TLV advertisements: enabled or disabled.
ETS TLV Statistic: Input Conf TLV pkts	Number of ETS Configuration TLVs received.
ETS TLV Statistic: Output Conf TLV pkts	Number of ETS Configuration TLVs transmitted.
ETS TLV Statistic: Error Conf TLV pkts	Number of ETS Error Configuration TLVs received.

Example (Summary)

```
Dell(conf)# show interfaces te 0/0 ets summary
Interface TenGigabitEthernet 0/0
```

```
Max Supported TC Groups is 4
Number of Traffic Classes is 8
Admin mode is on
Admin Parameters:
------------------
Admin is enabled
TC-grp Priority#        Bandwidth TSA
0      0,1,2,3,4,5,6,7  100%      ETS
1                         0%      ETS
2                         0%      ETS
3                         0%      ETS
4                         0%      ETS
5                         0%      ETS
6                         0%      ETS
7                         0%      ETS
Priority#              Bandwidth  TSA
0                        13%      ETS
1                        13%      ETS
2                        13%      ETS
3                        13%      ETS
4                        12%      ETS
5                        12%      ETS
6                        12%      ETS
7                        12%      ETS
Remote Parameters:
-------------------
Remote is disabled
Local Parameters:
------------------
Local is enabled
TC-grp Priority#        Bandwidth TSA
0      0,1,2,3,4,5,6,7  100%      ETS
1                         0%      ETS
2                         0%      ETS
3                         0%      ETS
4                         0%      ETS
5                         0%      ETS
6                         0%      ETS
7                         0%      ETS
Priority#               Bandwidth TSA
0                        13%      ETS
1                        13%      ETS
2                        13%      ETS
3                        13%      ETS
4                        12%      ETS
5                        12%      ETS
6                        12%      ETS
7                        12%      ETS
Oper status is init
Conf TLV Tx Status is disabled
Traffic Class TLV Tx Status is disabled
```

Example (Detail)

```
Dell(conf)# show interfaces tengigabitethernet 0/0 ets detail
Interface TenGigabitEthernet 0/0
Max Supported TC Groups is 4
Number of Traffic Classes is 8
Admin mode is on
Admin Parameters :
------------------
Admin is enabled
TC-grp Priority#        Bandwidth TSA
0      0,1,2,3,4,5,6,7  100%      ETS
1                       0%        ETS
```

```
2                       0%        ETS
3                       0%        ETS
4                       0%        ETS
5                       0%        ETS
6                       0%        ETS
7                       0%        ETS

Priority#               Bandwidth TSA
0                       13%       ETS
1                       13%       ETS
2                       13%       ETS
3                       13%       ETS
4                       12%       ETS
5                       12%       ETS
6                       12%       ETS
7                       12%       ETS
Remote Parameters:
-------------------
Remote is disabled

Local Parameters :
------------------
Local is enabled
TC-grp Priority#        Bandwidth TSA
0      0,1,2,3,4,5,6,7  100%      ETS
1                       0%        ETS
2                       0%        ETS
3                       0%        ETS
4                       0%        ETS
5                       0%        ETS
6                       0%        ETS
7                       0%        ETS

Priority#               Bandwidth TSA
0                       13%       ETS
1                       13%       ETS
2                       13%       ETS
3                       13%       ETS
4                       12%       ETS
5                       12%       ETS
6                       12%       ETS
7                       12%       ETS
Oper status is init
Conf TLV Tx Status is disabled
Traffic Class TLV Tx Status is disabled
0 Input Conf TLV Pkts, 0 Output Conf TLV Pkts, 0 Error Conf
TLV Pkts
0 Input Traffic Class TLV Pkts, 0 Output Traffic Class TLV
Pkts, 0 Error Traffic Class
TLV
Pkts
```

show interface pfc

Displays the PFC configuration applied to ingress traffic on an interface, including priorities and link delay.

Syntax `show interface` *`port-type slot/port pfc`* `{summary | detail}`

Parameters

port-type slot/ port pfc	Enter the port-type slot and port PFC information.

{summary | detail}	Enter the keyword `summary` for a summary list of results or enter the keyword `detail` for a full list of results.

Command Modes INTERFACE

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To clear the PFC TLV counters, use the `clear pfc counters interface` *`port-type slot/port`* command.

The following describes the `show interface pfc summary` command shown in the following example.

Field	Description
Interface	Interface type with stack-unit and port number.
Admin mode is on Admin is enabled	PFC admin mode is on or off with a list of the configured PFC priorities. When the PFC admin mode is on, PFC advertisements are enabled to be sent and received from peers; received PFC configuration take effect. The admin operational status for a DCBX exchange of PFC configuration is enabled or disabled.
Remote is enabled, Priority list Remote Willing Status is enabled	Operational status (enabled or disabled) of peer device for DCBX exchange of PFC configuration with a list of the configured PFC priorities. Willing status of peer device for DCBX exchange (Willing bit received in PFC TLV): enabled or disable.
Local is enabled	DCBX operational status (enabled or disabled) with a list of the configured PFC priorities.
Operational status (local port)	Port state for current operational PFC configuration: • `Init`: Local PFC configuration parameters were exchanged with the peer. • `Recommend`: Remote PFC configuration parameters were received from the peer. • `Internally propagated`: PFC configuration parameters were received from the configuration source.
PFC DCBX Oper status	Operational status for the exchange of the PFC configuration on the local port: match (up) or mismatch (down).

Field	Description
State Machine Type	Type of state machine used for DCBX exchanges of the PFC parameters: Feature — for legacy DCBX versions; Symmetric — for an IEEE version.
TLV Tx Status	Status of the PFC TLV advertisements: enabled or disabled.
PFC Link Delay	Link delay (in quanta) used to pause specified priority traffic.
Application Priority TLV: FCOE TLV Tx Status	Status of FCoE advertisements in application priority TLVs from the local DCBX port: enabled or disabled.
Application Priority TLV: SCSI TLV Tx Status	Status of ISCSI advertisements in application priority TLVs from the local DCBX port: enabled or disabled.
Application Priority TLV: Local FCOE Priority Map	Priority bitmap the local DCBX port uses in FCoE advertisements in application priority TLVs.
Application Priority TLV: Local ISCSI Priority Map	Priority bitmap the local DCBX port uses in ISCSI advertisements in application priority TLVs.
Application Priority TLV: Remote FCOE Priority Map	Status of FCoE advertisements in application priority TLVs from the remote peer port: enabled or disabled.
Application Priority TLV: Remote ISCSI Priority Map	Status of iSCSI advertisements in application priority TLVs from the remote peer port: enabled or disabled.
PFC TLV Statistics: Input TLV pkts	Number of PFC TLVs received.
PFC TLV Statistics: Output TLV pkts	Number of PFC TLVs transmitted.
PFC TLV Statistics: Error pkts	Number of PFC error packets received.
PFC TLV Statistics: Pause Tx pkts	Number of PFC pause frames transmitted.
PFC TLV Statistics: Pause Rx pkts	Number of PFC pause frames received.

Example (Summary)

```
Dell# show interfaces tengigabitethernet 0/49 pfc summary
Interface TenGigabitEthernet 0/49
  Admin mode is on
  Admin is enabled
  Remote is enabled, Priority list is 4
  Remote Willing Status is enabled
  Local is enabled
  Oper status is Recommended
  PFC DCBX Oper status is Up
  State Machine Type is Feature
  TLV Tx Status is enabled
  PFC Link Delay 45556 pause quantams
  Application Priority TLV Parameters :
  --------------------------------------
  FCOE TLV Tx Status is disabled
  ISCSI TLV Tx Status is disabled
  Local FCOE PriorityMap is 0x8
  Local ISCSI PriorityMap is 0x10
  Remote FCOE PriorityMap is 0x8
  Remote ISCSI PriorityMap is 0x8

Dell# show interfaces tengigabitethernet 0/49 pfc detail
  Interface TenGigabitEthernet 0/49
  Admin mode is on
  Admin is enabled
  Remote is enabled
  Remote Willing Status is enabled
  Local is enabled
  Oper status is recommended
  PFC DCBX Oper status is Up
  State Machine Type is Feature
  TLV Tx Status is enabled
  PFC Link Delay 45556 pause quanta
  Application Priority TLV Parameters :
  --------------------------------------
  FCOE TLV Tx Status is disabled
  ISCSI TLV Tx Status is disabled
  Local FCOE PriorityMap is 0x8
  Local ISCSI PriorityMap is 0x10
  Remote FCOE PriorityMap is 0x8
  Remote ISCSI PriorityMap is 0x8
  0 Input TLV pkts, 1 Output TLV pkts, 0 Error pkts,
  0 Pause Tx pkts, 0 Pause Rx pkts
```

show interface pfc statistics

Displays counters for the PFC frames received and transmitted (by dot1p priority class) on an interface.

Syntax `show interface port-type slot/port pfc statistics`

Parameters

port-type	Enter the port type.
slot/port	Enter the slot/port number.

Command Modes INTERFACE

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example (Summary)

```
Dell#show interfaces te 0/3 pfc statistics
Interface TenGigabitEthernet 0/3

Priority Rx XOFF Frames Rx Total Frames Tx Total Frames
```

```
--------------------------------------------------------
0        0              0               0
1        0              0               0
2        0              0               0
3        0              0               0
4        0              0               0
5        0              0               0
6        0              0               0
7        0              0               0
```

show qos dcb-input

Displays the PFC configuration in a DCB input policy.

Syntax `show qos dcb-input [pfc-profile]`

Parameters

pfc-profile	Enter the PFC profile.

Command Modes CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

NOTE: Please note that Dell Networking does not recommended to use this command as it has been deprecated in the current 9.4(0.0) release. A warning message appears when you try to run this command indicating that you have to use the `dcb-map` commands in the future.

Example

```
Dell(conf)# show qos dcb-input
dcb-input pfc-profile
  pfc link-delay 32
  pfc priority 0-1
dcb-input pfc-profile1
  no pfc mode on
  pfc priority 6-7
```

show qos dcb-output

Displays the ETS configuration in a DCB output policy.

Syntax `show qos dcb-output [ets-profile]`

Parameters

[ets-profile]	Enter the ETS profile.

Command Modes EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

NOTE: Please note that Dell Networking does not recommended to use this command as it has been deprecated in the current 9.4(0.0) release. A warning message appears when you try to run this command indicating that you have to use the `dcb-map` commands in the future.

Example

```
Dell# show qos dcb-output
dcb-output ets
  priority-group san qos-policy san
  priority-group ipc qos-policy ipc
  priority-group lan qos-policy lan
```

show qos priority-groups

Displays the ETS priority groups configured on the switch, including the 802.1p priority classes and ID of each group.

Syntax `show qos priority-groups`

Command Modes EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

NOTE: Please note that Dell Networking does not recommended to use this command as it has been deprecated in the current 9.4(0.0) release. A warning message appears when you try to run this command indicating that you have to use the `dcb-map` commands in the future.

Example

```
Dell#show qos priority-groups
priority-group ipc
  priority-list 4
  set-pgid 2
```

show stack-unit stack-ports ets details

Displays the ETS configuration applied to egress traffic on stacked ports, including ETS Operational mode on each unit and the configurated priority groups with dot1p priorities, bandwidth allocation, and scheduler type.

Syntax `show stack-unit {all | `*`stack-unit`*`} stack-ports {all | `*`port-number`*`} ets details`

Parameters

stack-unit	Enter the stack unit identification.
port-number	Enter the port number.

Command Modes CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell(conf)# show stack-unit all stack-ports all ets details

Stack unit 0 stack port all
Max Supported TC Groups is 4
Number of Traffic Classes is 1
Admin mode is on

Admin Parameters:
--------------------
Admin is enabled
TC-grp Priority#        Bandwidth TSA
------------------------------------------------
0      0,1,2,3,4,5,6,7  100%      ETS
1                       - -
2                       - -
3                       - -
4                       - -
5                       - -
6                       - -
7                       - -
8                       - -

Stack unit 1 stack port all
Max Supported TC Groups is 4
Number of Traffic Classes is 1
Admin mode is on
Admin Parameters:
--------------------
Admin is enabled
TC-grp Priority#        Bandwidth TSA
------------------------------------------------
0      0,1,2,3,4,5,6,7  100%      ETS
1                       -         -
2                       -         -
3                       -         -
4                       -         -
5                       -         -
6                       -         -
7                       -         -
8                       -         -
```

show stack-unit stack-ports pfc details

Displays the PFC configuration applied to ingress traffic on stacked ports, including PFC Operational mode on each unit with the configured priorities, link delay, and number of pause packets sent and received.

Syntax `show stack-unit {all | stack-unit} stack-ports {all | port-number} pfc details`

Parameters		
	stack-unit	Enter the stack unit.
	port-number	Enter the port number.

Command Modes CONFIGURATION

Command History		
	Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell(conf)# show stack-unit all stack-ports all pfc details

stack unit 0 stack-port all
  Admin mode is On
  Admin is enabled, Priority list is 4-5
  Local is enabled, Priority list is 4-5
  Link Delay 45556 pause quantum
  0 Pause Tx pkts, 0 Pause Rx pkts

stack unit 1 stack-port all
  Admin mode is On
  Admin is enabled, Priority list is 4-5
  Local is enabled, Priority list is 4-5
  Link Delay 45556 pause quantum
  0 Pause Tx pkts, 0 Pause Rx pkts
```

FIP Snooping

In a converged Ethernet network, an MXL Switch can operate as an intermediate Ethernet bridge to snoop on Fibre Channel over Ethernet initialization protocol (FIP) packets during the login process on Fibre Channel over Ethernet (FCoE) forwarders (FCFs).

Acting as a transit FIP snooping bridge, the switch uses dynamically-created ACLs to permit only authorized FCoE traffic to be transmitted between an FCoE end-device and an FCF. The following Dell Networking Operating System (OS) commands are used to configure and verify the FIP snooping feature.

clear fip-snooping database interface vlan

Clear FIP snooping information on a VLAN for a specified FCoE MAC address, ENode MAC address, or FCF MAC address, and remove the corresponding ACLs FIP snooping generates.

Syntax

```
clear fip-snooping database interface vlan vlan-id {fcoe-mac-address | enode-mac-address | fcf-mac-address}
```

Parameters		
	fcoe-mac-address	Enter the FCoE MAC address to be cleared of FIP snooping information.
	enode-mac-address	Enter the ENode MAC address to be cleared of FIP snooping information.

	fcf-mac-address	Enter the FCF MAC address to be cleared of FIP snooping information.
Command Modes	EXEC Privilege	
Command History	Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

clear fip-snooping statistics

Clears the statistics on the FIP packets snooped on all VLANs, a specified VLAN, or a specified port interface.

Syntax

```
clear fip-snooping statistics [interface vlan vlan-id |
interface port-type port/slot | interface port-channel port-
channel-number]
```

Parameters	*vlan-id*	Enter the VLAN ID of the FIP packet statistics to be cleared.
	port-type port/slot	Enter the port-type and slot number of the FIP packet statistics to be cleared.
	port-channel-number	Enter the port channel number of the FIP packet statistics to be cleared.
Command Modes	EXEC Privilege	
Command History	Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

feature fip-snooping

Enable FCoE transit and FIP snooping on a switch.

Syntax

```
feature fip-snooping
```

To disable the FCoE transit feature, use the `no feature fip-snooping` command.

Defaults: Disabled

Command Modes: CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

fip-snooping enable

Enable FIP snooping on all VLANs or on a specified VLAN.

Syntax

`fip-snooping enable`

To disable the FIP snooping feature on all or a specified VLAN, use the `no fip-snooping enable` command.

Defaults

FIP snooping is disabled on all VLANs.

Command Modes

- CONFIGURATION
- VLAN INTERFACE

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The maximum number of FCFs supported per FIP snooping-enabled VLAN is four. The maximum number of FIP snooping sessions supported per ENode server is 16.

fip-snooping fc-map

Configure the FC-MAP value FIP snooping uses on all VLANs.

Syntax

`fip-snooping fc-map fc-map-value`

To return the configured FM-MAP value to the default value, use the `no fip-snooping fc-map` command.

Parameters

fc-map-value	Enter the FC-MAP value FIP snooping uses. The range is from 0EFC00 to 0EFCFF.

Defaults

0x0EFC00

Command Modes

- CONFIGURATION
- VLAN INTERFACE

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

fip-snooping port-mode fcf

Configure the port for bridge-to-FCF links.

Syntax `fip-snooping port-mode fcf`

To disable the bridge-to-FCF link on a port, use the `no fip-snooping port-mode fcf` command.

Command Modes INTERFACE

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information The maximum number of FCFs supported per FIP snooping-enabled VLAN is four.

iSCSI Optimization

Internet small computer system interface (iSCSI) optimization enables quality-of-service (QoS) treatment for iSCSI storage traffic.

To configure and verify the iSCSI optimization feature, use the following Dell Networking Operating System (OS) commands.

advertise dcbx-app-tlv

Configure DCBX to send iSCSI TLV advertisements.

Syntax `advertise dcbx-app-tlv iscsi`

To disable DCBX iSCSI TLV advertisements, use the `no advertise dcbx-app-tlv iscsi` command.

Defaults Disabled.

Command Modes PROTOCOL LLDP

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information	You can configure iSCSI TLVs to send either globally or on a specified interface. The interface configuration takes priority over global configuration.

iscsi aging time

Set the aging time for iSCSI sessions.

Syntax

```
iscsi aging time time
```

To remove the iSCSI session aging time, use the `no iscsi aging time` command.

Parameters

time	Enter the aging time for the iSCSI session. The range is from 5 to 43,200 minutes.

Defaults **10 minutes**

Command Modes CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

iscsi cos

Set the QoS policy that is applied to the iSCSI flows.

Syntax

```
iscsi cos {enable | disable | dot1p vlan-priority-value
[remark] | dscp dscp-value [remark]}
```

To disable the QoS policy, use the `no iscsi cos dscp` command.

Parameters

enable	Enter the keyword `enable` to allow the application of preferential QoS treatment to iSCSI traffic so that the iSCSI packets are scheduled in the switch with a dot1p priority 4 regardless of the VLAN priority tag in the packet. The default is: the iSCSI packets are handled with dotp1 priority 4 without remark.
disable	Enter the keyword `disable` to disable the application of preferential QoS treatment to iSCSI frames.
dot1p *vlan-priority-value*	Enter the dot1p value of the VLAN priority tag assigned to the incoming packets in an iSCSI session. The range is from 0 to 7. The default is the dot1p value in ingress iSCSI frames is not changed and is the same priority is used in iSCSI TLV advertisements if you did not enter the `iscsi priority-bits` command.

dscp *dscp-value*	Enter the DSCP value assigned to the incoming packets in an iSCSI session. The valid range is from 0 to 63. The default is: the DSCP value in ingress packets is not changed.
remark	Marks the incoming iSCSI packets with the configured dot1p or DSCP value when they egress to the switch. The default is: the dot1and DSCP values in egress packets are not changed.

Defaults
The default dot1p VLAN priority value is 4 without the `remark` option.

Command Modes
CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

iscsi enable

Globally enable iSCSI optimization.

Syntax
`iscsi enable`

To disable iSCSI optimization, use the `no iscsi enable` command.

Parameters

enable	Enter the keyword `enable` to enable the iSCSI optimization feature.

Defaults
Disabled.

Command Modes
CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information
When you enable the iSCSI feature using the `iscsi enable` command, flow control settings are set to `rx on tx off` on all interfaces.

iscsi priority-bits

Configure the priority bitmap that advertises in the iSCSI application TLVs.

Syntax
`iscsi priority-bits`

To remove the configured priority bitmap, use the `no iscsi priority-bits` command.

Defaults	**4** (0x10 in the bitmap)
Command Modes	PROTOCOL LLDP (only on the global, not on the interface)
Command History	Version 9.2(0.0) — Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only. Version 8.3.16.1 — Introduced on the MXL 10/40GbE Switch IO Module.

iscsi profile-compellant

Configure the auto-detection of Dell Compellent arrays on a port.

Syntax	`iscsi profile-compellent`
Defaults	Dell Compellent disk arrays are not detected.
Command Modes	INTERFACE
Command History	Version 9.2(0.0) — Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only. Version 8.3.16.1 — Introduced on the MXL 10/40GbE Switch IO Module.

iscsi target port

Configure the iSCSI target ports and optionally, the IP addresses on which iSCSI communication is monitored.

Syntax	`iscsi target port [`*`tcp-port-2...tcp-port-16`*`]ip-address [`*`ip-address`*`]` To remove the configured iSCSI target ports or IP addresses, use the `no iscsi target port` command.
Parameters	*tcp-port-2...tcpport - 16* — Enter the tcp-port number of the iSCSI target ports. The `tcp-port-n` is the TCP port number or a list of TCP port numbers on which the iSCSI target listens to requests. Separate port numbers with a comma. The default is **860, 3260**. ip-address — (Optional) Enter the ip-address that the iSCSI monitors. The ip-address specifies the IP address of the iSCSI target.
Defaults	**860, 3260**
Command Modes	CONFIGURATION

Command History	**Version 9.2(0.0)**	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

You can configure up to 16 target TCP ports on the switch in one command or multiple commands.

When you use the `no iscsi target port` command and the TCP port you wish to delete is one bound to a specific IP address, the IP address value must be included in the command.

Interfaces

The commands in this chapter are supported by Dell Networking Operating System (OS).

This chapter contains the following sections:

- Basic Interface Commands
- Port Channel Commands

Basic Interface Commands

The following commands are for Physical interfaces.

clear counters

Clear the counters used in the `show interfaces` commands for all virtual router redundancy protocol (VRRP) groups, virtual local area networks (VLANs), and physical interfaces, or selected ones.

Syntax `clear counters` *`interface`*

Parameters

interface	(OPTIONAL) Enter any of the following keywords and slot/port or number to clear counters from a specified interface: • For the management interface on the stack-unit, enter the keyword `management ethernet` followed by slot/port information. The slot and port range is 0. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information. • For a Port Channel interface, enter the keyword port-channel followed by a number. Range: 1-128

Defaults Without an interface specified, the command clears all interface counters.

Command Modes EXEC Privilege

Command History		
	Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#clear counters
Clear counters on all interfaces [confirm]
```

Related Commands

mac learning-limit — allows aging of MACs even though a learning-limit is configured or disallow station move on learned MACs.

show interfaces — displays information on the interfaces.

description

Assign a descriptive text string to the interface.

Syntax

`description desc_text`

To delete a description, use the `no description` command.

Parameters		
	desc_text	Enter a text string up to 240 characters long. To use special characters as a part of the description string, you must enclose the whole string in double quotes.

Defaults

none

Command Modes

INTERFACE

Command History		
	Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Important Points to Remember:

- Spaces between characters are not preserved after entering this command unless you enclose the entire description in quotation marks (“*desc_text*”).
- Entering a text string after the `description` command overwrites any previous text string that you previously configured as the description.
- The `shutdown` and `description` commands are the only commands that you can configure on an interface that is a member of a port-channel.
- Use the `show interfaces description` command to display descriptions configured for each interface.

Related Commands

show interfaces description — displays the description field of the interfaces.

flowcontrol

Control how the system responds to and generates 802.3x pause frames on 10G and 40Gig stack units.

Syntax

```
flowcontrol rx {off | on} tx {off | on} threshold
```

Parameters

rx on	Enter the keywords `rx on` to process the received flow control frames on this port. This is the default value for the receive side.
rx off	Enter the keywords `rx off` to ignore the received flow control frames on this port.
tx on	Enter the keywords `tx on` to send control frames from this port to the connected device when a higher rate of traffic is received. This is the default value on the send side.
tx off	Enter the keywords `tx off` so that flow control frames are not sent from this port to the connected device when a higher rate of traffic is received.

Defaults

- `rx off`
- `tx off`

Command Modes

INTERFACE

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The globally assigned 48-bit Multicast address 01-80-C2-00-00-01 is used to send and receive pause frames. To allow full-duplex flow control, stations implementing the pause operation instruct the MAC to enable the reception of frames with a destination address equal to this multicast address.

The pause:

- Starts when *either* the packet pointer or the buffer threshold is met (whichever is met first). When the discard threshold is met, packets are dropped.
- Ends when *both* the packet pointer and the buffer threshold fall below 50% of the threshold settings.

The *discard threshold* defines when the interface starts dropping the packet on the interface. This may be necessary when a connected device does not honor the flow control frame sent by the switch. The discard threshold should be larger than the *buffer threshold* so that the buffer holds at least hold at least three packets.

On 4–port 10G stack units: Changes in the flow-control values may not be reflected automatically in the `show interface` output for 10G interfaces. This is because 10G interfaces do not support auto-negotiation.

Important Points to Remember

- Do not enable `tx pause` when buffer carving is enabled. For information and assistance, consult Dell Networking TAC.
- Asymmetric flow control (`rx on tx off`, or `rx off tx on`) setting for the interface port less than 100 Mb/s speed is not permitted. The following error is returned:

  `Can’t configure Asymmetric flowcontrol when speed <1G, config ignored`
- The only configuration applicable to half duplex ports is `rx off tx off`. The following error is returned:

  `Cannot configure Asymmetric flowcontrol when speed <1G, config ignored>`
- You cannot configure half duplex when the flow control configuration is on (default is `rx on tx on`). The following error is returned: `Cannot configure half duplex when flowcontrol is on, config ignored`

NOTE: The flow control must be off (`rx off tx off`) before configuring the half duplex.

Example (partial)

```
Dell(conf-if-tengig-0/1)#show config
!
interface TenGigabitEthernet 0/1
no ip address
switchport
no negotiation auto
flowcontrol rx off tx on
no shutdown
...
```

Example (Values)

This Example shows how the Dell Networking OS negotiates the flow control values between two Dell Networking chassis connected back-to-back using 1G copper ports.

```
Configured

LocRxConf LocTxConf RemoteRxConf RemoteTxConf
off       off         off           off
                      off           on
                      on            off
                      on            on

off       on          off           off
                      off           on
                      on            off
                      on            on

on        off         off           off
                      off           on
                      on            off
                      on            on

on        on          off           off
```

```
                     off           on
                     on            off
                     on            on

LocNegRx LocNegTx RemNegRx RemNegTx
off      off     off      off
off      off     off      off
off      off     off      off
off      off     off      off

off      off     off      off
off      off     off      off
off      on      on       off
off      off     off      off

off      off     off      off
on       off     off      on
on       on      on       on
on       on      on       on

off      off       off     off
off      off       off     off
on       on        on      on
on       on        on      on
```

Related Commands

show running-config — displays the flow configuration parameters (non-default values only).

show interfaces — displays the negotiated flow control parameters.

interface

Configure a physical interface on the switch.

Syntax `interface interface`

Parameters

interface	Enter one of the following keywords and slot/port or number information: • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a Fibre Channel interface, enter the keyword `FibreChannel`, then the slot/port information.

Defaults Not configured.

Command Modes CONFIGURATION

Command History

Version 9.4(0.0)	Added the support for interfaces.
Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.

Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

You cannot delete a physical interface.

By default, physical interfaces are disabled (`shutdown`) and are in Layer 3 mode. To place an interface in mode, ensure that the interface’s configuration does not contain an IP address and enter the `Port Channel Commands` command.

The tunnel interface operates as an ECMP (equal cost multi path) only when the next hop to the tunnel destination is over a physical interface. If you select any other interface as the next hop to the tunnel destination, the tunnel interface does not operate as an ECMP.

Example

```
Dell(conf)#interface tengig 0/0
Dell(conf-if-tengig-0/0)#exit#
```

Related Commands

interface port-channel — configures a port channel.

interface vlan — configures a VLAN.

show interfaces — displays the interface configuration.

interface ManagementEthernet

Configure the Management port on the system.

Syntax

`interface ManagementEthernet slot/port`

Parameters

slot/port	Enter the keyword `ManagementEthernet`, then the slot number (0 or 1) and port number zero (0).

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

You cannot delete a Management port.

The Management port is enabled by default (`no shutdown`). To assign an IP address to the Management port, use the `ip address` command.

Example

```
Dell(conf)#interface managementethernet 0/0
Dell(conf-if-ma-0/0)#
```

interface range

This command permits configuration of a range of interfaces to which subsequent commands are applied (bulk configuration). Using the `interface range` command, you can enter identical commands for a range of interface.

Syntax

```
interface range interface, interface,...
```

Parameters

interface, interface,...	Enter the keywords `interface range` and one of the interfaces — slot/port, port-channel, or VLAN number. Select the range of interfaces for bulk configuration. You can enter up to six comma-separated ranges. Spaces are not required between the commas. Comma-separated ranges can include VLANs, port-channels, and physical interfaces. Slot/Port information must contain a space before and after the dash. For example, `interface range gigabitethernet 0/1 - 5` is valid; `interface range gigabitethernet 0/1-5` is NOT valid. • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

Defaults

none

Command Modes

CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

When creating an interface range, interfaces appear in the order they are entered; they are not sorted. The command verifies that interfaces are present (physical) or configured (logical).

Important Points to Remember:

- Bulk configuration is created if at least one interface is valid.
- Non-existing interfaces are excluded from the bulk configuration with a warning message.
- The `interface range` prompt includes interface types with slot/port information for valid interfaces. The prompt allows for a maximum of 32

characters. If the bulk configuration exceeds 32 characters, it is represented by an ellipsis (...).

- When the `interface range` prompt has multiple port ranges, the smaller port range is excluded from the prompt.
- If overlapping port ranges are specified, the port range is extended to the smallest start port and the biggest end port.

Example (Bulk)

```
Dell(conf)#interface range so 2/0-1, te 10/0, gi 3/0, fa 0/0
% Warning: Non-existing ports (not configured) are ignored by
interface-range
```

Example (Multiple Ports)

```
Dell(conf)#interface range gi 2/0 - 23, gi 2/1 - 10
Dell(conf-if-range-gi-2/0-23#
```

Example (Overlapping Ports)

```
Dell(conf)#interface range gi 2/1 - 11, gi 2/1 - 23
Dell(conf-if-range-gi-2/1-23#
```

Usage Information

Only VLAN and port-channel interfaces created using the `interface vlan` and `interface port-channel` commands can be used in the `interface range` command.

Use the `show running-config` command to display the VLAN and port-channel interfaces. VLAN or port-channel interfaces that are not displayed in the `show running-config` command cannot be used with the bulk configuration feature of the `interface range` command. You cannot create virtual interfaces (VLAN, Port-channel) using the `interface range` command.

NOTE: If a range has VLAN, physical, port-channel, and SONET interfaces, only commands related to physical interfaces can be bulk configured. To configure commands specific to VLAN or port-channel, only those respective interfaces should be configured in a particular range.

Example (Single Range)

This example shows a single range bulk configuration.

```
Dell(config)# interface range gigabitethernet 5/1 - 23
Dell(config-if-range)# no shutdown
Dell(config-if-range)#
```

Example (Multiple Range)

This example shows how to use commas to add different interface types to the range enabling all Gigabit Ethernet interfaces in the range 5/1 to 5/23 and both Ten-Gigabit Ethernet interfaces 1/1 and 1/2.

```
Dell(config-if)# interface range gigabitethernet5/1-23,
tengigabitethernet1/1-2
Dell(config-if-range)# no shutdown
Dell(config-if-range)#
```

Example (Multiple Range)

This example shows how to use commas to add SONET, VLAN, and port-channel interfaces to the range.

```
Dell(config-if)# interface range gigabitethernet5/1-23,
tengigabitethernet1/1−2,
Vlan 2-100, Port 1-25
Dell(config-if-range)# no shutdown
Dell(config-if-range)#
```

Related Commands

[interface port-channel](#) — configures a port channel group.

[interface vlan](#) — configures a VLAN interface.

[show config (from INTERFACE RANGE mode)](#) — shows the bulk configuration interfaces.

[show range](#) — shows the bulk configuration ranges.

interface vlan

Configure a VLAN. You can configure up to 4096 VLANs.

Syntax

`interface vlan vlan-id`

To delete a VLAN, use the `no interface vlan vlan-id` command.

Parameters

vlan-id	Enter a number as the VLAN Identifier. The range is from 1 to 4096.

Defaults

Not configured, except for the Default VLAN, which is configured as VLAN 1.

Command Modes

CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

For more information about VLANs and the commands to configure them, refer to the Virtual LAN (VLAN) Commands.

FTP, TFTP, and SNMP operations are not supported on a VLAN. MAC/IP ACLs are not supported.

Example

```
Dell(conf)#int vlan 3
Dell(conf-if-vl-3)#
```

Related Commands

[interface](#) — configures a physical interface.

[interface port-channel](#) — configures a port channel group.

intf-type cr4 autoneg

Set the interface type as CR4 with auto-negotiation enabled.

Syntax

`intf-type cr4 autoneg`

If you configure `intf-type cr4 autoneg`, use the `no intf-type cr4 autoneg` command to set the interface type as cr4 with autonegotiation disabled.

Defaults

Not configured

Command Modes

CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

If you configure `interface type` as CR4 with auto-negotiation enabled, also configure CR4 with auto-negotiation. Many DAC cable link issues are resolved by setting the interface type as CR4.

Related Commands

interface — configures a physical interface.

interface port-channel — configures a port channel group.

keepalive

Send keepalive packets periodically to keep an interface alive when it is not transmitting data.

Syntax

`keepalive [seconds]`

To stop sending keepalive packets, use the `no keepalive` command.

Parameters

seconds	(OPTIONAL) For interfaces with PPP encapsulation enabled, enter the number of seconds between keepalive packets. The range is from 0 to 23767. The default is **10 seconds**.

Defaults

Enabled.

Command Modes

INTERFACE

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information	When you configure `keepalive`, the system sends a self-addressed packet out of the configured interface to verify that the far end of a WAN link is up. When you configure `no keepalive`, the system does not send keepalive packets and so the local end of a WAN link remains up even if the remote end is down.

mtu

Set the link maximum transmission unit (MTU) (frame size) for an Ethernet interface.

Syntax

`mtu *value*`

To return to the default MTU value, use the `no mtu` command.

Parameters

value	Enter a maximum frame size in bytes. The range is from 594 to 9252. MXL Switch Range is from 594 to 12000. The default is **1554**.

Defaults **1554**

Command Modes INTERFACE

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

If the packet includes a Layer 2 header, the difference between the link MTU and IP MTU (`ip mtu` command) must be enough bytes to include the Layer 2 header.

- The IP MTU is adjusted automatically when you configure the Layer 2 MTU with the `mtu` command.

When you enter the `no mtu` command, The Dell Networking OS reduces the IP MTU value to 1536 bytes.

Link MTU and IP MTU considerations for port channels and VLANs are as follows.

port channels:

- All members must have the same link MTU value and the same IP MTU value.
- The port channel link MTU and IP MTU must be less than or equal to the link MTU and IP MTU values configured on the channel members. For example, if the members have a link MTU of 2100 and an IP MTU 2000, the port channel's MTU values cannot be higher than 2100 for link MTU or 2000 bytes for IP MTU.

VLANs:

- All members of a VLAN must have same IP MTU value.
- Members can have different Link MTU values. Tagged members must have a link MTU 4 bytes higher than untagged members to account for the packet tag.
- The VLAN link MTU and IP MTU must be less than or equal to the link MTU and IP MTU values configured on the VLAN members. For example, the VLAN

contains tagged members with Link MTU of 1522 and IP MTU of 1500 and untagged members with Link MTU of 1518 and IP MTU of 1500. The VLAN's Link MTU cannot be higher than 1518 bytes and its IP MTU cannot be higher than 1500 bytes.

The following shows the difference between Link MTU and IP MTU.

Layer 2 Overhead	Link MTU and IP MTU Delta
Ethernet (untagged)	18 bytes
VLAN Tag	22 bytes
Untagged Packet with VLAN-Stack Header	22 bytes
Tagged Packet with VLAN-Stack Header	26 bytes

negotiation auto

Enable auto-negotiation on an interface.

Syntax	`negotiation auto` To disable auto-negotiation, use the `no negotiation auto` command.
Defaults	Enabled.
Command Modes	INTERFACE

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The `no negotiation auto` command is only available if you first manually set the speed of a port to **10Mbits** or **100Mbits**.

The `negotiation auto` command provides a `mode` option for configuring an individual port to forced-master/forced slave after you enable auto-negotiation.

If you do not use the `mode` option, the default setting is **slave**. If you do not configure forced-master or forced-slave on a port, the port negotiates to either a master or a slave state. Port status is one of the following:

- Forced-master
- Force-slave
- Master

- Slave
- Auto-neg Error — typically indicates that both ends of the node are configured with forced-master or forced-slave.

CAUTION: Ensure that one end of your node is configured as forced-master and one is configured as forced-slave. If both are configured the same (that is, forced-master or forced-slave), the `show interfaces` command flaps between an auto-neg-error and forced-master/slave states.

You can display master/slave settings with the `show interfaces` command.

Example (Master/Slave)

```
Dell(conf)# int tengig 0/0
Dell(conf-if)#neg auto
Dell(conf-if-autoneg)# ?

end         Exit from configuration mode
exit        Exit from autoneg configuration mode
mode        Specify autoneg mode
no          Negate a command or set its defaults
show        Show autoneg configuration information
Dell(conf-if-autoneg)#mode ?
forced-master Force port to master mode
forced-slave Force port to slave mode
Dell(conf-if-autoneg)#
```

Example (Master/Slave, partial)

```
Dell#show interfaces configured
TenGigabitEthernet 13/18 is up, line protocol is up
Hardware is Dell Force10Eth, address is 00:01:e8:05:f7:fc
   Current address is 00:01:e8:05:f7:fc
Interface index is 474791997
Internet address is 1.1.1.1/24
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed 1000 Mbit, Mode full duplex, Master
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interfaces" counters 00:12:42
Queueing strategy: fifo
Input Statistics:
...
```

User Information

Both sides of the link must have auto-negotiation enabled or disabled for the link to come up.

The following details the possible speed and auto-negotiation combinations for a line between two 10/100/1000 Base-T Ethernet interfaces.

Port 0

- auto-negotiation enabled* speed 1000 or auto
- auto-negotiation enabled speed 100
- auto-negotiation disabled speed 100
- auto-negotiation disabled speed 100
- auto-negotiation enabled* speed 1000 or auto

Port 1

- auto-negotiation enabled* speed 1000 or auto
- auto-negotiation enabled speed 100
- auto-negotiation disabled speed 100
- auto-negotiation enabled speed 100
- auto-negotiation disabled speed 100

Link Status Between Port 1 and Port 2

- Up at 1000 Mb/s
- Up at 100 Mb/s
- Up at 100 Mb/s
- Down
- Down

* You cannot disable auto-negotiation when the speed is set to 1000 or auto.

Related Commands

speed (for 1000/10000 interfaces) — sets the link speed to 1000, 10000, or auto-negotiate the speed.

portmode hybrid

To accept *both* tagged and untagged frames, set a physical port or port-channel. A port configured this way is identified as a hybrid port in report displays.

Syntax

`portmode hybrid`

To return a port to accept *either* tagged or untagged frames (non-hybrid), use the `no portmode hybrid` command.

Defaults

non-hybrid

Command Modes

INTERFACE (conf-if-*interface-slot/port*)

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The following describes the `interface` command shown in the following example. This example sets a port as hybrid, makes the port a tagged member of VLAN 20, and an untagged member of VLAN 10, which becomes the native VLAN of the port. The port now accepts:

- untagged frames and classify them as VLAN 10 frames
- VLAN 20 tagged frames

The following describes the `do show interfaces` command shown in the following example. This example shows output with “Hybrid” as the newly added value for 802.1QTagged. The options for this field are:

- True — port is tagged
- False — port is untagged
- Hybrid — port accepts both tagged and untagged frames

The following describes the `interface vlan` command shown in the following example. This example shows unconfiguration of the hybrid port using the `no portmode hybrid` command.

NOTE: Remove all other configurations on the port before you can remove the hybrid configuration from the port.

Example

```
Dell(conf)#interface tengig 0/20
Dell(conf-if-te-0/20)#no shut
Dell(conf-if-te-0/20)#portmode hybrid
Dell(conf-if-te-0/20)#sw
Dell(conf-if-te-0/20)#int vlan 10
Dell(conf-if-vl-10)#tag tengig 0/20
Dell(conf-if-vl-10)#int vlan 20
Dell(conf-if-vl-20)#untag tengig 0/20
Dell(conf-if-vl-20)#
```

Example (tagged hybrid)

```
Dell(conf)#interface tengig 0/20
Dell(conf-if-te-0/20)#no shut
Dell(conf-if-te-0/20)#portmode hybrid
Dell(conf-if-te-0/20#sw
Dell(conf-if-te-0/20)#int vlan 10
Dell(conf-if-vl-10)#int tengig 0/20
Dell(conf-if-vl-20)# untag tengig 0/20

Dell (conf-if-vl-20)#

Dell(conf)#do show interfaces switchport tengigabitethernet
3/20

Codes: U - Untagged, T - Tagged
       x - Dot1x untagged, X - Dot1x tagged
       G - GVRP tagged, M - Trunk, H - VSN tagged
       i - Internal untagged, I - Internal tagged, v - VLT
untagged,
       V - VLT tagged

Name: TenGigabitEthernet 3/20

802.1QTagged: Hybrid
Vlan membership:
Q   Vlans
U   20
T   10

Native VlanId: 20.

Dell(conf)#
```

Example (unconfigure the hybrid port)

```
Dell(conf-if-vl-20)#interface vlan 10
Dell(conf-if-vl-10)#no untagged tengig 0/20
Dell(conf-if-vl-10)#interface vlan 20
Dell(conf-if-vl-20)#no tagged tengig 0/20
Dell(conf-if-vl-20)#interface tengig 0/20
Dell(conf-if-te-0/20)#no portmode hybrid
Dell(conf-if-vl-20)#
```

Related Commands

show interfaces switchport — displays the configuration of switchport (Layer 2) interfaces on the switch.

vlan-stack trunk — specifies an interface as a trunk port to the Stackable VLAN network.

stack-unit portmode

Split a single 40G port into 4-10G ports on the MXL switch.

Syntax

`stack-unit stack-unit port number portmode quad`

Parameters

stack-unit	Enter the stack member unit identifier of the stack member to reset. The range is 0 to 5. NOTE: The MXL switch commands accept Unit ID numbers from 0 to 5, though the MXL switch supports stacking up to three units only with the Dell Networking OS version 8.3.7.1.
number	Enter the port number of the 40G port to be split. Enter one of the following port numbers for the MXL switch: 48, 52, 56, or 60.

Defaults

Disabled.

Command Modes

CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Splitting a 40G port into 4x10G port is supported on standalone and stacked units.

- You cannot use split ports as stack-link to stack an MXL Switch.
- The split ports MXL switch unit cannot be a part of any stacked system.
- The unit number with the split ports must be the default (stack-unit 0).
- This set up can be verified using `show system brief` command. If the unit ID is different than 0, it must be renumbered to 0 before ports are split by using the `stackunit id renumber 0` command in EXEC mode.

The quad port must be in a default configuration before it can be split into 4x10G ports. The 40G port is lost in the config when the port is split, so be sure that the port is also removed from other L2/L3 feature configurations.

The system must be reloaded after issuing the CLI for the change to take effect.

Port Channel Commands

A link aggregation group (LAG) is a group of links that appear to a MAC client as if they were a single link according to IEEE 802.3ad. In the Dell Networking OS, a LAG is referred to as a Port Channel.

- For the MXL switch, the maximum port channel ID is 128 and the maximum members per port channel is 16.

Because each port can be assigned to only one Port Channel, and each Port Channel must have at least one port, some of those nominally available Port Channels might have no function because they could have no members if there are not enough ports installed. In the MXL 10/40GbE Switch IO Module, those ports could be provided by stack members.

NOTE: The Dell Networking OS implementation of LAG or Port Channel requires that you configure a LAG on both switches manually. For information about Dell Networking OS link aggregation control protocol (LACP) for dynamic LAGs, refer to the *Link Aggregation Control Protocol (LACP)* chapter. For more information about configuring and using Port Channels, refer to the *Dell Networking OS Configuration Guide*.

channel-member

Add an interface to the Port Channel, while in INTERFACE PORTCHANNEL mode.

Syntax

`channel-member interface`

To delete an interface from a Port Channel, use the `no channel-member interface` command.

Parameters

interface	(OPTIONAL) Enter any of the following keywords and slot/port or number information: • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

Defaults

Not configured.

Command Modes

INTERFACE PORTCHANNEL

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Use the `interface port-channel` command to access this command.

You cannot add an interface to a Port Channel if the interface contains an IP address in its configuration.

Link MTU and IP MTU considerations for Port Channels are:

- All members must have the same link MTU value and the same IP MTU value.
- The Port Channel link MTU and IP MTU must be less than or equal to the link MTU and IP MTU values configured on the channel members. For example, if the members have a link MTU of 2100 and an IP MTU 2000, the Port Channel's MTU values cannot be higher than 2100 for link MTU or 2000 bytes for IP MTU.

When an interface is removed from a Port Channel with the `no channel-member` command, the interface reverts to its configuration prior to joining the Port Channel.

An interface can belong to only one Port Channel.

You can add up to 16 interfaces to a Port Channel on the MXL switch. The interfaces can be located on different line cards but must be the same physical type and speed (for example, all 10-Gigabit Ethernet interfaces). However, you can combine 100/1000 interfaces and GE interfaces in the same Port Channel.

If the Port Channel contains a mix of interfaces with 100 Mb/s speed and 1000 Mb/s speed, the software disables those interfaces whose speed does not match the speed of the first interface configured and enabled in the Port Channel. If that first interface goes down, the Port Channel does not change its designated speed; disable and re-enable the Port Channel or change the order of the channel members configuration to change the designated speed. If the Port Channel contains a mix of interfaces with 100 Mb/s speed and 1000 Mb/s speed, the software disables those interfaces whose speed does not match the speed of the first interface configured and enabled in the Port Channel. If that first interface goes down, the Port Channel does not change its designated speed; disable and re-enable the Port Channel or change the order of the channel members configuration to change the designated speed. For more information about Port Channels, refer to the *Dell Networking OS Configuration Guide*.

Related Commands	description — assigns a descriptive text string to the interface. interface port-channel — creates a Port Channel interface. shutdown — disables/enables the port channel.

interface port-channel

Create a Port Channel interface, which is a link aggregation group (LAG) containing 16 physical interfaces on the XML switch.

Syntax	`interface port-channel` *`channel-number`* To delete a Port Channel, use the `no interface port-channel` *`channel-number`* command.

Parameters

channel-number	For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Port Channel interfaces are logical interfaces and can be either in Layer 2 mode (by using the `switchport` command) or Layer 3 mode (by configuring an IP address). You can add a Port Channel in Layer 2 mode to a VLAN.

A Port Channel can contain both 100/1000 interfaces and GE interfaces. Based on the first interface configured in the Port Channel and enabled, the Dell Networking OS determines if the Port Channel uses 100 Mb/s or 1000 Mb/s as the common speed. For more information, refer to channel-member.

If the line card is in a Jumbo mode chassis, you can also configure the `mtu` and `ip mtu` commands. The Link MTU and IP MTU values configured on the channel members must be greater than the Link MTU and IP MTU values configured on the Port Channel interface.

NOTE: In a Jumbo-enabled system, you must configure all members of a Port Channel with the same link MTU values and the same IP MTU values.

Example

```
Dell(conf)#int port-channel 2
Dell(conf-if-po-2)#
```

Related Commands

channel-member — adds a physical interface to the LAG.

interface — configures a physical interface.

interface vlan — configures a VLAN.

shutdown — disables/enables the port channel.

minimum-links

Configure the minimum number of links in a LAG (Port Channel) that must be in “oper up” status for the LAG to be also in “oper up” status.

Syntax

`minimum-links` *`number`*

Parameters

number	Enter the number of links in a LAG that must be in “oper up” status. The range is from 1 to 16. The default is **1**.

Defaults	**1**
Command Modes	INTERFACE

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information	If you use this command to configure the minimum number of links in a LAG that must be in “oper up” status, the LAG must have at least that number of “oper up” links before it can be declared as up. For example, if the required minimum is four, and only three are up, the LAG is considered down.

Internet Group Management Protocol (IGMP)

The IGMP commands are supported by the Dell Networking operating software on the Aggregator.

This chapter contains the following sections:

- IGMP Commands
- IGMP Snooping Commands

IGMP Commands

Dell Networking OS supports IGMPv1/v2/v3 and is compliant with RFC-3376.

Important Points to Remember

- IGMPv2 is the default version of IGMP on interfaces. You can configure IGMPv3 on interfaces. It is backward compatible with IGMPv2.
- There is no hard limit on the maximum number of groups supported.
- IGMPv3 router interoperability with IGMPv2 and IGMPv1 routers on the same subnet is not supported.
- An administrative command (`ip igmp version`) is added to manually set the IGMP version.
- All commands previously used for IGMPv2 are compatible with IGMPv3.

ip igmp group-join-limit

To limit the number of IGMP groups that can be joined in a second, use this feature.

Syntax	`ip igmp group-join-limit` *`number`*

Parameters

number	Enter the number of IGMP groups permitted to join in a second. The range is from 1 to 10000.

Defaults	none

Command Modes	CONFIGURATION (conf-if-*interface-slot/port*)
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 9.0.2.0	Introduced on the S6000.
Version 8.3.19.0	Introduced on the S4820T.
Version 8.3.11.1	Introduced on the Z9000.
Version 8.3.7.0	Introduced on the S4810.
Version 7.8.1.0	Introduced on the C-Series and S-Series.
Version 7.6.1.0	Introduced on the E-Series.

ip igmp querier-timeout

Change the interval that must pass before a multicast router decides that there is no longer another multicast router that should be the querier.

Syntax

```
ip igmp querier-timeout seconds
```

To return to the default value, use the `no ip igmp querier-timeout` command.

Parameters

seconds	Enter the number of seconds the router must wait to become the new querier. The range is from 60 to 300. The default is **125 seconds**.

Defaults	**125 seconds**
Command Modes	INTERFACE
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 9.0.2.0	Introduced on the S6000.
Version 8.3.19.0	Introduced on the S4820T.

Version 8.3.11.1	Introduced on the Z9000.
Version 8.3.7.0	Introduced on the S4810.
Version 7.8.1.0	Introduced on the S-Series.
Version 7.7.1.0	Introduced on the C-Series.
Version 7.6.1.0	Introduced on the S-Series in Interface VLAN mode only to enable the system to act as an IGMP Proxy Querier.
Version 7.5.1.0	Introduced on the C-Series in Interface VLAN mode only to enable the system to act as an IGMP Proxy Querier.
E-Series legacy command.	

ip igmp query-interval

Change the transmission frequency of IGMP general queries the Querier sends.

Syntax

`ip igmp query-interval *seconds*`

To return to the default values, use the `no ip igmp query-interval` command.

Parameters

seconds	Enter the number of seconds between queries sent out. The range is from 1 to 18000. The default is **60 seconds**.

Defaults **60 seconds**

Command Modes INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 9.0.2.0	Introduced on the S6000.
Version 8.3.19.0	Introduced on the S4820T.
Version 8.3.11.1	Introduced on the Z9000.
Version 8.3.7.0	Introduced on the S4810.
Version 7.8.1.0	Introduced on the S-Series.
Version 7.7.1.0	Introduced on the C-Series.
Version 7.6.1.0	Introduced on the S-Series in Interface VLAN mode only to enable the system to act as an IGMP Proxy Querier.

Version 7.5.1.0	Introduced on the C-Series in Interface VLAN mode only to enable the system to act as an IGMP Proxy Querier.
E-Series legacy command.	

ip igmp query-max-resp-time

Set the maximum query response time advertised in general queries.

Syntax

```
ip igmp query-max-resp-time seconds
```

To return to the default values, use the `no ip igmp query-max-resp-time` command.

Parameters

seconds	Enter the number of seconds for the maximum response time. The range is from 1 to 25. The default is **10 seconds**.

Defaults **10 seconds**

Command Modes INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 9.0.2.0	Introduced on the S6000.
Version 8.3.19.0	Introduced on the S4820T.
Version 8.3.11.1	Introduced on the Z9000.
Version 8.3.7.0	Introduced on the S4810.
Version 7.6.1.0	Introduced on the S-Series.
Version 7.5.1.0	Introduced on the C-Series.
Version 7.6.1.0	Introduced on the S-Series in Interface VLAN mode only to enable the system to act as an IGMP Proxy Querier.
Version 7.5.1.0	Introduced on the C-Series in Interface VLAN mode only to enable the system to act as an IGMP Proxy Querier.
E-Series legacy command.	

ip igmp version

Manually set the version of the router to IGMPv2 or IGMPv3.

Syntax `ip igmp version {2 | 3}`

Parameters

2	Enter the number 2 to set the IGMP version number to IGMPv2.
3	Enter the number 3 to set the IGMP version number to IGMPv3.

Defaults **2** (that is, IGMPv2)

Command Modes INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version 9.0.2.0	Introduced on the S6000.
Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.19.0	Introduced on the S4820T.
Version 8.3.11.1	Introduced on the Z9000.
Version 8.3.7.0	Introduced on the S4810.
Version 7.8.1.0	Introduced on the S-Series.
Version 7.7.1.0	Introduced on the C-Series.
Version 7.5.1.0	Introduced on the E-Series.

IGMP Snooping Commands

Dell Networking OS supports IGMP Snooping version 2 and 3 on all Dell Networking systems.

Important Points to Remember for IGMP Snooping

- Dell Networking OS supports version 1, version 2, and version 3 hosts.
- Dell Networking OS IGMP snooping implementation is based on IP multicast address (not based on Layer 2 multicast mac address) and the IGMP snooping entries are in Layer 3 flow table not in Layer 2 forwarding information base (FIB).
- Dell Networking OS IGMP snooping implementation is based on draft-ietf-magma-snoop-10.
- Dell Networking OS supports IGMP snooping on JUMBO-enabled cards.
- IGMP snooping is not enabled by default on the switch.
- A maximum of 1800 groups and 600 VLAN are supported.

- IGMP snooping is not supported on a default VLAN interface.
- IGMP snooping is not supported over VLAN-Stack-enabled VLAN interfaces (you must disable IGMP snooping on a VLAN interface before configuring VLAN-Stack-related commands).

ip igmp snooping enable

Enable IGMP snooping on all or a single VLAN. This command is the master on/off switch to enable IGMP snooping.

Syntax

```
ip igmp snooping enable
```

To disable IGMP snooping, use the `no ip igmp snooping enable` command.

Defaults

Disabled.

Command Modes

- CONFIGURATION
- INTERFACE VLAN

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 9.0.2.0	Introduced on the S6000.
Version 8.3.19.0	Introduced on the S4820T.
Version 8.3.11.1	Introduced on the Z9000.
Version 8.3.7.0	Introduced on the S4810.
Version 7.6.1.0	Introduced on the S-Series.
Version 7.5.1.0	Introduced on the C-Series.

Usage Information

To enable IGMP snooping, enter this command. When you enable this command from CONFIGURATION mode, IGMP snooping enables on all VLAN interfaces (except the default VLAN).

NOTE: Execute the `no shutdown` command on the VLAN interface for IGMP Snooping to function.

ip igmp snooping fast-leave

Enable IGMP snooping fast-leave for this VLAN.

Z9000 S4810 S4820TS6000

Syntax

```
ip igmp snooping fast-leave
```

To disable IGMP snooping fast leave, use the `no igmp snooping fast-leave` command.

Defaults Not configured.

Command Modes INTERFACE VLAN — (conf-if-vl-*n*)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 9.0.2.0	Introduced on the S6000.
Version 8.3.19.0	Introduced on the S4820T.
Version 8.3.11.1	Introduced on the Z9000.
Version 8.3.7.0	Introduced on the S4810.
Version 7.6.1.0	Introduced on the S-Series.
Version 7.5.1.0	Introduced on the C-Series.
E-Series legacy command.	

Usage Information Queriers normally send some queries when a leave message is received prior to deleting a group from the membership database. There may be situations when you require a fast deletion of a group. When you enable IGMP fast leave processing, the switch removes an interface from the multicast group as soon as it detects an IGMP version 2 leave message on the interface.

ip igmp snooping last-member-query-interval

The last member query interval is the maximum response time inserted into Group-Specific queries sent in response to Group-Leave messages.

Z9000 S4810 S4820TS6000

Syntax

```
ip igmp snooping last-member-query-interval milliseconds
```

To return to the default value, use the `no ip igmp snooping last-member-query-interval` command.

Parameters

milliseconds	Enter the interval in milliseconds. The range is from 100 to 65535. The default is **1000 milliseconds**.

Defaults **1000 milliseconds**

Command Modes INTERFACE VLAN

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 9.0.2.0	Introduced on the S6000.
Version 8.3.19.0	Introduced on the S4820T.
Version 8.3.11.1	Introduced on the Z9000.
Version 8.3.7.0	Introduced on the S4810.
Version 7.6.1.0	Introduced on the S-Series.
Version 7.5.1.0	Introduced on the C-Series.
E-Series legacy command	

Usage Information

This last-member-query-interval is also the interval between successive Group-Specific Query messages. To change the last-member-query interval, use this command.

ip igmp snooping mrouter

Statically configure a VLAN member port as a multicast router interface.

Z9000 S4810 S4820TS6000

Syntax

`ip igmp snooping mrouter interface interface`

To delete a specific multicast router interface, use the `no igmp snooping mrouter interface interface` command.

Parameters

interface *interface*	Enter the following keywords and slot/port or number information: • For a 100/1000 Ethernet interface, enter the keyword `gigabitethernet` followed by the slot/port information. • For a 1-Gigabit Ethernet interface, enter the keyword `gigabitethernet` followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a Port Channel interface, enter the keywords `port-channel` then a number. For the C-Series and S-Series, the range is from 1 to 128.

Defaults	Not configured.
Command Modes	INTERFACE VLAN — (conf-if-vl-*n*)
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*. The following is a list of the Dell Networking OS version history for this command.

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 9.0.2.0	Introduced on the S6000.
Version 8.3.19.0	Introduced on the S4820T.
Version 8.3.11.1	Introduced on the Z9000.
Version 8.3.7.0	Introduced on the S4810.
Version 7.6.1.0	Introduced on the S-Series.
Version 7.5.1.0	Introduced on the C-Series.
E-Series legacy command.	

Usage Information

Dell Networking OS provides the capability of statically configuring the interface to which a multicast router is attached. To configure a static connection to the multicast router, enter the `ip igmp snooping mrouter interface` command in the VLAN context. The interface to the router must be a part of the VLAN where you are entering the command.

ip igmp snooping querier

Enable IGMP querier processing for the VLAN interface.

Z9000 S4810 S4820TS6000

Syntax	`ip igmp snooping querier` To disable IGMP querier processing for the VLAN interface, use the `no ip igmp snooping querier` command.
Defaults	Not configured.
Command Modes	INTERFACE VLAN — (conf-if-vl-*n*)
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*. The following is a list of the Dell Networking OS version history for this command.

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 9.0.2.0	Introduced on the S6000.
Version 8.3.19.0	Introduced on the S4820T.
Version 8.3.11.1	Introduced on the Z9000.
Version 8.3.7.0	Introduced on the S4810.
Version 7.6.1.0	Introduced on the S-Series.
Version 7.5.1.0	Introduced on the C-Series.
E-Series legacy command	

Usage Information

This command enables the IGMP switch to send General Queries periodically. This behavior is useful when there is no multicast router present in the VLAN because the multicast traffic is not routed. Assign an IP address to the VLAN interface for the switch to act as a querier for this VLAN.

Layer 2

This chapter describes commands to configure Layer 2 features.

This chapter contains:

- MAC Addressing Commands

MAC Addressing Commands

The following commands are related to configuring, managing, and viewing MAC addresses.

mac-address-table aging-time

Specify an aging time for MAC addresses to remove from the MAC address table.

Syntax

`mac-address-table aging-time` *`seconds`*

To delete the configured aging time, use the `no mac-address-table aging-time` *`seconds`* command.

Parameters

seconds	Enter either zero (0) or a number as the number of seconds before MAC addresses are relearned. To disable aging of the MAC address table, enter `0`. The range is from 10 to 1000000. The default is **1800 seconds**.

Defaults

1800 seconds

Command Modes	CONFIGURATION	
Command History	Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

mac-address-table static

Associate specific MAC or hardware addresses to an interface and virtual local area networks (VLANs).

Syntax

`mac-address-table static` *`mac-address`* `output` *`interface`* `vlan` *`vlan-id`*

To remove a MAC address, use the `no mac-address-table static` *`mac-address`* `output` *`interface`* `vlan` *`vlan-id`* command.

Parameters

mac-address	Enter the 48-bit hexadecimal address in nn:nn:nn:nn:nn:nn format.
output *interface*	Enter the keyword `output` then one of the following interfaces for which traffic is forwarded: • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
vlan *vlan-id*	Enter the keyword `vlan` then a VLAN ID number from 1 to 4094.

Defaults	Not configured.	
Command Modes	CONFIGURATION	
Command History	Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

mac-address-table station-move refresh-arp

Ensure that address resolution protocol (ARP) refreshes the egress interface when a station move occurs due to a topology change.

Syntax

`[no] mac-address-table station-move refresh-arp`

Defaults	none	
Command Modes	CONFIGURATION	
Command History	**Version 9.2(0.0)**	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	For details about using this command, refer to the “NIC Teaming” section of the Layer 2 chapter in the *Dell Networking OS Configuration Guide*.	

Link Aggregation Control Protocol (LACP)

This chapter contains commands for Dell Networks’s implementation of the link aggregation control protocol (LACP) for creating dynamic link aggregation groups (LAGs) — known as port-channels in the Dell Networking Operating System (OS).

NOTE: For static LAG commands, refer to the Interfaces chapter), based on the standards specified in the IEEE 802.3 Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications.

lacp long-timeout

Configure a long timeout period (30 seconds) for an LACP session.

Syntax	`lacp long-timeout` To reset the timeout period to a short timeout (1 second), use the `no lacp long-timeout` command.	
Defaults	**1 second**	
Command Modes	INTERFACE (conf-if-po-number)	
Command History	**Version 9.2(0.0)**	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	This command applies to dynamic port-channel interfaces only. When applied on a static port-channel, this command has no effect.	

lacp port-priority

To influence which ports will be put in Standby mode when there is a hardware limitation that prevents all compatible ports from aggregating, configure the port priority.

Syntax

`lacp port-priority` *`priority-value`*

To return to the default setting, use the `no lacp port-priority` *`priority-value`* command.

Parameters

priority-value	Enter the port-priority value. The higher the value number, the lower the priority. The range is from 1 to 65535. The default is **32768**.

Defaults

32768

Command Modes

INTERFACE

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

port-channel mode

Configure the LACP port channel mode.

Syntax

`port-channel` *`number`* `mode [active] [passive] [off]`

Parameters

number	Enter the keywords `number` then a number.
active	Enter the keyword `active` to set the mode to the active state. NOTE: LACP modes are defined in *Usage Information*.
passive	Enter the keyword `passive` to set the mode to the passive state. NOTE: LACP modes are defined in *Usage Information*.
off	Enter the keyword `off` to set the mode to the off state. NOTE: LACP modes are defined in *Usage Information*.

Defaults

off

Command Modes

INTERFACE

Command History		
	Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

LACP Modes

Mode	Function
active	An interface is in an active negotiating state in this mode. LACP runs on any link configured in the active state and also automatically initiates negotiation with other ports by initiating LACP packets.
passive	An interface is not in an active negotiating state in this mode. LACP runs on any link configured in the passive state. Ports in a passive state respond to negotiation requests from other ports that are in active states. Ports in a passive state respond to LACP packets
off	An interface cannot be part of a dynamic port channel in off mode. LACP does not run on a port configured in off mode.

port-channel-protocol lacp

Enable LACP on any LAN port.

Syntax

```
port-channel-protocol lacp
```

To disable LACP on a LAN port, use the `no port-channel-protocol lacp` command.

Command Modes

INTERFACE

Command History		
	Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
	Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell(conf)#interface TenGigabitethernet 3/15
Dell(conf-if-tengig-3/15)#no shutdown
Dell(conf-if-tengig-3/15)#port-channel-protocol lacp
Dell(conf-if-tengig-3/15-lacp)#port-channel 32 mode active
...
Dell(conf)#interface TenGigabitethernet 3/16
Dell(conf-if-tengig-3/16)#no shutdown
Dell(conf-if-tengig-3/16)#port-channel-protocol lacp
Dell(conf-if-tengig-3/16-lacp)#port-channel 32 mode active
```

Link Layer Discovery Protocol (LLDP)

Link layer discovery protocol (LLDP) advertises connectivity and management from the local station to the adjacent stations on an IEEE 802 LAN.

LLDP facilitates multi-vendor interoperability by using standard management tools to discover and make available a physical topology for network management. The Dell Networking operating software implementation of LLDP is based on IEEE standard 801.1ab.

The starting point for using LLDP is invoking LLDP with the `protocol lldp` command in either CONFIGURATION or INTERFACE mode.

The information LLDP distributes is stored by its recipients in a standard management information base (MIB). You can access the information by a network management system through a management protocol such as simple network management protocol (SNMP).

For details about implementing LLDP/LLDP-MED, refer to the Link Layer Discovery Protocol chapter of the *Dell Networking OS Configuration Guide*.

advertise dot3-tlv

Advertise dot3 TLVs (Type, Length, Value).

Syntax

```
advertise dot3-tlv {max-frame-size}
```

To remove advertised dot3-tlv, use the `no advertise dot3-tlv {max-frame-size}` command.

Parameters

max-frame-size	Enter the keywords `max-frame-size` to advertise the dot3 maximum frame size.

Defaults none

Command Modes CONFIGURATION (conf-lldp) and INTERFACE (conf-if-*interface*-lldp)

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

advertise management-tlv

Advertise management TLVs (Type, Length, Value).

Syntax

```
advertise management-tlv {system-capabilities | system-description | system-name}
```

To remove advertised management TLVs, use the `no advertise management-tlv {system-capabilities | system-description | system-name}` command.

Parameters

system-capabilities	Enter the keywords `system-capabilities` to advertise the system capabilities TLVs to the LLDP peer.
system-description	Enter the keywords `system-description` to advertise the system description TLVs to the LLDP peer.
system-name	Enter the keywords `system-name` to advertise the system name TLVs to the LLDP peer.

Defaults none

Command Modes CONFIGURATION (conf-lldp)

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information The command options `system-capabilities`, `system-description`, and `system-name` can be invoked individually or together, in any sequence.

clear lldp counters

Clear LLDP transmitting and receiving counters for all physical interfaces or a specific physical interface.

Syntax `clear lldp counters` *`interface`*

Parameters

interface	Enter the following keywords and slot/port or number information: • For a 10-Gigabit Ethernet interface, enter the keyword `tenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

Defaults none

Command Modes EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

clear lldp neighbors

Clear LLDP neighbor information for all interfaces or a specific interface.

Syntax

```
clear lldp neighbors {interface}
```

Parameters

interface	Enter the following keywords and slot/port or number information: • For a 10-Gigabit Ethernet interface, enter the keyword `tenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

Defaults

none

Command Modes

EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

debug lldp interface

To display timer events, neighbor additions or deletions, and other information about incoming and outgoing packets, enable LLDP debugging.

Syntax

```
debug lldp interface {interface | all}{events | packet {brief |
detail} {tx | rx | both}}
```

To disable debugging, use the `no debug lldp interface {interface | all}{events} {packet {brief | detail} {tx | rx | both}}` command.

Parameters

interface	Enter the following keywords and slot/port or number information: • For a 10-Gigabit Ethernet interface, enter the keyword `tenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
all	(OPTIONAL) Enter the keyword `all` to display information on all interfaces.
events	(OPTIONAL) Enter the keyword `events` to display major events such as timer events.

packet	(OPTIONAL) Enter the keyword `packet` to display information regarding packets coming in or going out.
brief	(OPTIONAL) Enter the keyword `brief` to display brief packet information.
detail	(OPTIONAL) Enter the keyword `detail` to display detailed packet information.
tx	(OPTIONAL) Enter the keyword `tx` to display transmit-only packet information.
rx	(OPTIONAL) Enter the keyword `rx` to display receive-only packet information.
both	(OPTIONAL) Enter the keyword `both` to display both receive and transmit packet information.

Defaults none

Command Modes EXEC Privilege

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

disable

Enable or disable LLDP.

Syntax `disable`

To enable LLDP, use the `no disable` command.

Defaults Enabled, that is `no disable`.

Command Modes CONFIGURATION (conf-lldp) and INTERFACE (conf-if-*interface*-lldp)

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

protocol lldp (Configuration) — enables LLDP globally.

debug lldp interface — debugs LLDP.

show lldp neighbors — displays the LLDP neighbors.

hello

Configure the rate at which the LLDP control packets are sent to its peer.

Syntax	`hello seconds` To revert to the default, use the `no hello seconds` command.
Parameters	*seconds*: Enter the rate, in seconds, at which the control packets are sent to its peer. The rate is from 5 to 180 seconds. The default is **30 seconds**.
Defaults	**30 seconds**
Command Modes	CONFIGURATION (conf-lldp) and INTERFACE (conf-if-*interface*-lldp)
Command History	Version 9.2(0.0): Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only. Version 8.3.16.1: Introduced on the MXL 10/40GbE Switch IO Module.

multiplier

Set the number of consecutive misses before LLDP declares the interface dead.

Syntax	`multiplier integer` To return to the default, use the `no multiplier integer` command.
Parameters	*integer*: Enter the number of consecutive misses before the LLDP declares the interface dead. The range is from 2 to 10.
Defaults	**4 x hello**
Command Modes	CONFIGURATION (conf-lldp) and INTERFACE (conf-if-*interface*-lldp)
Command History	Version 9.2(0.0): Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only. Version 8.3.16.1: Introduced on the MXL 10/40GbE Switch IO Module.

Quality of Service (QoS)

The Dell Networking operating software commands for quality of service (QoS) include traffic conditioning and congestion control. QoS commands are not universally supported on all Dell Networking Products.

Per-Port QoS Commands

Per-port QoS (port-based QoS) allows you to define the QoS configuration on a per-physical-port basis.

dot1p-priority

Assign a value to the IEEE 802.1p bits on the traffic this interface receives.

Syntax

`dot1p-priority priority-value`

To delete the IEEE 802.1p configuration on the interface, use the `no dot1p-priority` command.

Parameters

priority-value	Enter a value from 0 to 7.

dot1p	Queue Number
0	0
1	0
2	0
3	1
4	2
5	3
6	3
7	3

Defaults none

Command Modes INTERFACE

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The `dot1p-priority` command changes the priority of incoming traffic on the interface. The system places traffic marked with a priority in the correct queue and processes that traffic according to its queue.

When you set the priority for a port channel, the physical interfaces assigned to the port channel are configured with the same value. You cannot assign the `dot1p-priority` command to individual interfaces in a port channel.

service-class dynamic dot1p

Honor all 802.1p markings on incoming switched traffic on an interface (from INTERFACE mode) or on all interfaces (from CONFIGURATION mode). A CONFIGURATION mode entry supersedes an INTERFACE mode entry.

Syntax

`service-class dynamic dot1p`

To return to the default setting, use the `no service-class dynamic dot1p` command.

Defaults

All dot1p traffic is mapped to Queue 0 unless you enable the `service-class dynamic dot1p` command. The default mapping is as follows:

dot1p	Queue ID
0	0
1	0
2	0
3	1
4	2
5	3
6	3
7	3

Command Modes

- INTERFACE
- CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To honor all incoming 802.1p markings on incoming switched traffic on the interface, enter this command. By default, this facility is not enabled (that is, the 802.1p markings on incoming traffic are not honored).

You can apply this command on both physical interfaces and port channels. When you set the service-class dynamic for a port channel, the physical interfaces assigned to the port channel are automatically configured; you cannot assign the `service-class dynamic` command to individual interfaces in a port channel.

- All dot1p traffic is mapped to Queue 0 unless you enable the `service-class dynamic dot1p` command on an interface or globally.
- Layer 2 or Layer 3 service policies supersede dot1p service classes.

service-class dot1p-mapping

Configure a service-class criterion based on a dot1p value.

Syntax

```
service-class dot1p-mapping {dot1p0 value | dot1p1 value |
dot1p2 queue | dot1p3 value | dot1p4 value| dot1p5 value |
dot1p6 value | dot1p7 value}
```

Parameters

value	Enter a dot1p list number and value. The list number range is from 0 to 7. The range is from 0 to 3.

Defaults

For each dot1p Priority, the default CoS queue value is:

- dot1p CoS Queue

  0 0-7

  1 0-7

  2 0-7

  3 0-7

  4 0-7

  5 0-7

  6 0-7

  7 0-7

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 9.0.2.0	Introduced on the S6000.

Version 8.3.19.0	Introduced on the S4820T.
Version 8.3.11.1	Introduced on the Z9000.
Version 8.3.7.0	Introduced on the S4810.

Usage Information To apply dot1p-queue-mapping, use the `service-class dynamic dot1p` command.

Related Commands service-class dot1p-mapping — displays the dot1p priority to queue mapping on the switch.

service-class bandwidth-percentage

Specify a minimum bandwidth for queues.

Syntax `service-class bandwidth-percentage queue0 number queue1 number queue2 number queue3 number`

Parameters

number	Enter the bandwidth-weight, as a percentage. The range is from 1 to 100.

Defaults none

Command Modes CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information Guarantee a minimum bandwidth to different queues globally using the `service-class bandwidth-percentage` command from CONFIGURATION mode. The command is applied in the same way as the `bandwidth-percentage` command in an output QoS policy. The `bandwidth-percentage` command in QOS-POLICY-OUT mode supersedes the `service-class bandwidth-percentage` command.

When you enable ETS, the egress QoS features in the output QoS policy-map (such as `service-class bandwidth-percentage` and `bandwidth-percentage`), the default bandwidth allocation ratio for egress queues are superseded by ETS configurations. This is to provide compatibility with DCBX. Therefore, Dell Networking OS recommends disabling ETS when you wish to apply these features exclusively. After you disable ETS on an interface, the configured parameters are applied.

Policy-Based QoS Commands

Policy-based traffic classification is handled with class maps. These maps classify unicast traffic into one of four classes. The system allows you to match multiple class maps and specify multiple match criteria. Policy-based QoS is not supported on logical interfaces, such as port-channels, VLANs, or Loopbacks.

bandwidth-percentage

Assign a percentage of weight to the class/queue.

Syntax	`bandwidth-percentage` *`percentage`* To remove the bandwidth percentage, use the `no bandwidth-percentage` command.
Parameters	*percentage* — Enter the percentage assignment of weight to the class/queue. The range is from 1 to 100% (granularity 1%).
Defaults	none
Command Modes	CONFIGURATION (conf-qos-policy-out)
Command History	Version 9.2(0.0) — Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only. Version 8.3.16.1 — Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	The unit of bandwidth percentage is 1%. If the sum of the bandwidth percentages given to all eight classes exceeds 100%, the bandwidth percentage automatically scales down to 100%.
Related Commands	qos-policy-output — creates a QoS output policy.

description

Add a description to the selected policy map or QoS policy.

Syntax	`description {`*`description`*`}` To remove the description, use the `no description {`*`description`*`}` command.
Parameters	*description* — Enter a description to identify the policies (80 characters maximum).
Defaults	none

Command Modes	CONFIGURATION (policy-map-input and policy-map-output; conf-qos-policy-in and conf-qos-policy-out; wred)

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

policy-map-output — creates an output policy map.

qos-policy-output — creates an output QoS-policy on the router.

policy-aggregate

Allow an aggregate method of configuring per-port QoS via policy maps. An aggregate QoS policy is part of the policy map (input/output) applied on an interface.

Syntax

```
policy-aggregate qos-policy-name
```

To remove a policy aggregate configuration, use the `no policy-aggregate qos-policy-name` command.

Parameters

qos-policy-name	Enter the name of the policy map in character format (32 characters maximum).

Defaults: none

Command Modes: CONFIGURATION (policy-map-input and policy-map-output)

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Aggregate input/output QoS policy applies to all the port ingoing/outgoing traffic. Aggregate input/output QoS policy can coexist with per queue input/output QoS policies.

1. If only aggregate input QoS policy exists, input traffic conditioning configurations (rate-police) apply. Any marking configurations in aggregate input QoS policy are ignored.
2. If aggregate input QoS policy and per class input QoS policy coexist, aggregate input QoS policy preempts per class input QoS policy on input traffic conditioning (rate-police). In other words, if rate police configuration exists in the aggregate QoS policy, the rate police configurations in per class QoS are ignored. Marking configurations in per class input QoS policy still apply to each queue.

Related Commands	policy-map-output — creates an output policy map.

policy-map-output

Create an output policy map.

Syntax

`policy-map-output policy-map-name`

To remove a policy map, use the `no policy-map-output policy-map-name` command.

Parameters

policy-map-name	Enter the name for the policy map in character format (32 characters maximum).

Defaults none

Command Modes CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To assign traffic to different flows using QoS policy, use the Output Policy map. This command enables Policy-Map-Output Configuration mode (conf-policy-map-out).

Related Commands

service-queue — assigns a class map and QoS policy to different queues.

policy-aggregate — allows an aggregate method of configuring per-port QoS using policy maps.

service-policy output — applies an output policy map to the selected interface.

qos-policy-output

Create a QoS output policy.

Syntax

`qos-policy-output qos-policy-name`

To remove an existing output QoS policy, use the `no qos-policy-output qos-policy-name` command.

Parameters

qos-policy-name	Enter your output QoS policy name in character format (32 characters maximum).

Defaults none

Command Modes	CONFIGURATION
Command History	**Version 8.3.16.1** — Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	To specify the name of the output QoS policy, use this command. After the output policy is specified, rate-limit, bandwidth-percentage, and WRED can be defined. This command enables Qos-Policy-Output Configuration mode — (conf-qos-policy-out).
Related Commands	bandwidth-percentage — assigns weight to the class/queue percentage.

service-policy output

Apply an output policy map to the selected interface.

Syntax

```
service-policy output policy-map-name
```

To remove the output policy map from the interface, use the `no service-policy output policy-map-name` command.

Parameters

policy-map-name	Enter the name for the policy map in character format (16 characters maximum). You can identify an existing policy map or name one that does not yet exist.

Defaults: none

Command Modes: INTERFACE

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

A single policy-map can be attached to one or more interfaces to specify the service-policy for those interfaces. A policy map attached to an interface can be modified.

Related Commands

policy-map-output — creates an output policy map.

service-queue

Assign a class map and QoS policy to different queues.

Syntax

```
service-queue queue-id [class-map class-map-name] [qos-policy
qos-policy-name]
```

To remove the queue assignment, use the `no service-queue` *`queue-id`* `[class-map` *`class-map-name`*`] [qos-policy` *`qos-policy-name`*`]` command.

Parameters

queue-id	Enter the value used to identify a queue. The range is from 0 to 3 (four queues per interface; four queues are reserved for control traffic).
class-map *class-map-name*	(OPTIONAL) Enter the keyword `class-map` then the class map name assigned to the queue in character format (32 character maximum). NOTE: This option is available under `policy-map-input` only.
qos-policy *qos-policy-name*	(OPTIONAL) Enter the keywords `qos-policy` then the QoS policy name assigned to the queue in text format (32 characters maximum). This specifies the input QoS policy assigned to the queue under `policy-map-input` and output QoS policy under `policy-map-output` context.

Defaults

none

Command Modes

CONFIGURATION (conf-policy-map-in and conf-policy-map-out)

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

There are four queues per interface on the MXL switch. This command assigns a class map or QoS policy to different queues.

Related Commands

service-policy output — applies an output policy map to the selected interface.

show qos qos-policy-output

View the output QoS policy details.

Syntax

`show qos qos-policy-output [`*`qos-policy-name`*`]`

Parameters

qos-policy-name	Enter the QoS policy name.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History	**Version 8.3.16.1**	Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Dell#show qos qos-policy-output

Qos-policy-output qmap_out
Bandwidth-percentage 10
Qos-policy-output qmap_wg
Rate-shape 100 50
Wred yellow wy
Wred green wg
Dell#
```

Virtual Link Trunking (VLT)

VLT allows physical links between two chassis to appear as a single virtual link to the network core. VLT eliminates the requirement for Spanning Tree protocols by allowing link aggregation group (LAG) terminations on two separate distribution or core switches, and by supporting a loop-free topology. VLT provides Layer 2 multipathing, creating redundancy through increased bandwidth and enabling multiple parallel paths between nodes and load-balancing traffic where alternative paths exist.

NOTE: When you launch the VLT link, the VLT peer-ship is not established if any of the following is **TRUE**:

- The VLT System-MAC configured on both the VLT peers do not match.
- The VLT Unit-Id configured on both the VLT peers are identical.
- The VLT System-MAC or Unit-Id is configured only on one of the VLT peers.
- The VLT domain ID is not the same on both peers.

If the VLT peer-ship is already established, changing the System-MAC or Unit-Id does not cause VLT peer-ship to go down.

Also, if the VLT peer-ship is already established and the VLT Unit-Id or System-MAC are configured on both peers, then changing the CLI configurations on the VLT Unit-Id or System-MAC is rejected if any of the following become **TRUE**:

- After making the CLI configuration change, the VLT Unit-Id becomes identical on both peers.
- After making the CLI configuration change, the VLT System-MAC do not match on both peers.

When the VLT peer-ship is already established, you can remove the VLT Unit-Id or System-MAC configuration from either or both peers. However, removing configuration settings can cause the VLT ports to go down if you configure the Unit-Id or System-MAC on only one of the VLT peers.

back-up destination

Configure the IPv4 or IPv6 address of the management interface on the remote VLT peer to be used as the endpoint of the VLT backup link for sending out-of-band hello messages.

Syntax

```
back-up destination {[ipv4-address] | [ipv6 ipv6-address]
[interval seconds]}
```

Parameters

ipv4–address	Enter the IPv4 address of the backup destination.
ipv6	Enter the keyword `ipv6` then an IPv6 address in the X:X:X:X::X format.
interval *seconds*	Enter the keyword `interval` to specify the time interval to send hello messages. The range is from 1 to 5 seconds. The default is 1 second.

Defaults **1 second**

Command Modes VLT DOMAIN

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 9.2(0.2)	Added support for IPv6.
Version 9.0.2.0	Introduced on the S6000.
Version 9.0.0.0	Introduced on the Z9000.
Version 8.3.19.0	Introduced on the S4820T.
Version 8.3.8.0	Introduced on the S4810.

clear vlt statistics

Clear the statistics on VLT operations.

Syntax

```
clear vlt statistics [arp | domain | igmp-snoop | mac |
multicast | ndp]
```

Parameters

domain	Clear the VLT statistics for the domain.
multicast	Clear the VLT statistics for multicast.
mac	Clear the VLT statistics for the MAC address.
arp	Clear the VLT statistics for ARP.
igmp-snoop	Clear the VLT statistics for IGMP snooping.
ndp	Clear the VLT statistics for NDP.

Command Modes EXEC

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 9.2(0.2)	Added `multicast` and `ndp` parameters.
Version 9.0.2.0	Introduced on the S6000.
Version 9.0.0.0	Introduced on the Z9000.
Version 8.3.19.0	Introduced on the S4820T.
Version 8.3.12.0	Introduced on the S4810.

Example

```
VLT ARP Statistics
----------------
ARP Tunnel Pkts sent:0
ARP Tunnel Pkts Rcvd:0
ARP-sync Pkts Sent:0
ARP-sync Pkts Rcvd:0
ARP Reg Request sent:19
ARP Reg Request rcvd:10
```

lacp ungroup member-independent

Prevent possible loop during the bootup of a VLT peer switch or a device that accesses the VLT domain.

Syntax

```
lacp ungroup member-independent {vlt | port-channel}
```

Parameters

port-channel	Force all LACP port-channel members to become switchports.
vlt	Force all VLT LACP members to become switchports.

Defaults Not configured.

Command Modes CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 9.0.2.0	Introduced on the S6000.

Version 9.0.0.0	Introduced on the Z9000.
Version 8.3.19.0	Introduced on the S4820T.
Version 8.3.12.0	Added port-channel parameter on the S4810.
Version 8.3.8.0	Introduced on the S4810.

Usage Information

LACP on the VLT ports (on a VLT switch or access device), which are members of the virtual link trunk, is not brought up until the VLT domain is recognized on the access device.

On the S4810, during boot-up in a stacking configuration, the system must be able to reach the DHCP server with the boot image and configuration image. During boot-up, only untagged DHCP requests are sent to the DHCP server to receive an offer on static LAGs between switches. The DHCP server must be configured to start in BMP mode. If switches are connected using LACP port-channels like the VLT peer and Top of Rack (ToR), use the **port-channel** parameter on the ToR-side configuration to allow member ports of an ungrouped LACP port-channel to inherit vlan membership of that port channel to ensure untagged packets that are sent by a VLT peer device reach the DHCP server located on the ToR.

To ungroup the VLT and port-channel configurations, use the **no lacp ungroup member independent** command on a VLT port channel, depending on whether the port channel is VLT or non-VLT.

Example

```
Dell(conf)#lacp ungroup member-independent ?
port-channel                LACP port-channel members become
switchports
vlt                                   All VLT LACP members
become switchports
```

peer-link port-channel

Configure the specified port channel as the chassis interconnect trunk between VLT peers in the domain.

Syntax

`peer-link port-channel` *`port-channel-number`* `{peer-down-vlan` *`vlan id`*`}`

Parameters

port-channel-number	Enter the port-channel number that acts as the interconnect trunk.
peer-down-vlan *vlan id*	Enter the keyword `peer-down-vlan` then a VLAN ID to configure the VLAN that the VLT peer link uses when the VLT peer is down.

Defaults

Not configured.

Command Modes

VLT DOMAIN

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 9.0.2.0	Introduced on the S6000.
Version 9.0.0.0	Introduced on the Z9000.
Version 8.3.19.0	Introduced on the S4820T.
Version 8.3.12.0	Added support for the **peer-down-vlan** parameter.
Version 8.3.8.0	Introduced on the S4810.

Usage Information

To configure the VLAN from where the VLT peer forwards packets received over the VLTi from an adjacent VLT peer that is down, use the **peer-down-vlan** parameter. When a VLT peer with bare metal provisioning (BMP) is booting up, it sends untagged DHCP discover packets to its peer over the VLTi. To ensure that the DHCP discover packets are forwarded to the VLAN that has the DHCP server, use this configuration.

show vlt mismatch

Display mismatches in VLT parameters.

Syntax

```
show vlt mismatch
```

Command Modes

EXEC

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 9.2(0.2)	Introduced on the Z9000, S4810, and S4820T.

Example

```
Dell#show vlt mismatch
Domain
-----------
Parameters        Local            Peer
------------     -----------      ---------
    Unit-ID       0                 15

Vlan-config
------------
Vlan-ID      Local Mode     Peer Mode
```

```
---------   ------------ -----------

     100             --                 L3

Vlan IPV4 Multicast Status
--------------------------
  Vlan-ID      Local Status       Peer Status
  --------     ------------       -----------

  4094              Active             Inactive

Dell#
```

system-mac

Reconfigure the default MAC address for the domain.

Syntax `system-mac mac-address`

Parameters

mac-address	Enter the system MAC address for the VLT domain.

Defaults Not configured.

Command Modes VLT DOMAIN

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 9.0.0.0	Introduced on the Z9000.
Version 8.3.19.0	Introduced on the S4820T.
Version 8.3.8.0	Introduced on the S4810.

Usage Information When you create a VLT domain on a switch, Dell Networking OS automatically creates a VLT-system MAC address used for internal system operations.

To reconfigure the default MAC address for the domain by entering a new MAC address in the format nn:nn:nn:nn:nn:nn, use the `system-mac` command.

You must also reconfigure the same MAC address on the VLT peer switch.

unit-id

Explicitly configure the default unit ID of a VLT peer switch.

Syntax `unit-id [0 | 1]`

Parameters		
	0 | 1	Configure the default unit ID of a VLT peer switch. Enter `0` for the first peer or enter `1` for the second peer.

Defaults Automatically assigned based on the MAC address of each VLT peer. The peer with the lower MAC address is assigned unit 0; the peer with the higher MAC address is assigned unit 1.

Command Modes VLT DOMAIN

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 9.0.2.0	Introduced on the S6000.
Version 9.0.0.0	Introduced on the Z9000.
Version 8.3.19.0	Introduced on the S4820T.
Version 8.3.8.0	Introduced on the S4810.

Usage Information When you create a VLT domain on a switch, Dell Networking OS automatically assigns a unique unit ID (0 or 1) to each peer switch. The unit IDs are used for internal system operations. Use the `unit-id` command to explicitly configure the unit ID of a VLT peer. Configure a different unit ID (0 or 1) on each peer switch.

To minimize the time required for the VLT system to determine the unit ID assigned to each peer switch when one peer reboots, use this command.

vlt domain

Enable VLT on a switch, configure a VLT domain, and enter VLT-domain configuration mode.

Syntax `vlt domain domain-id`

Parameters		
	domain-id	Enter the Domain ID number. Configure the same domain ID on the peer switch. The range of domain IDs is from 1 to 1000.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 9.0.2.0	Introduced on the S6000.
Version 9.0.0.0	Introduced on the Z9000.
Version 8.3.19.0	Introduced on the S4820T.
Version 8.3.8.0	Introduced on the S4810.

Usage Information

The VLT domain ID must be the same between the two VLT devices. If the domain ID is not the same, a syslog message is generated and VLT does not launch.

Related Commands

show vlt brief — uses the `show vlt brief` command to display the delay-restore value.

vlt-peer-lag port-channel

Associate the port channel to the corresponding port channel in the VLT peer for the VLT connection to an attached device.

Syntax

`vlt-peer-lag port-channel id-number`

Parameters

id-number	Enter the respective vlt port-channel number of the peer device.

Defaults

Not configured.

Command Modes

INTERFACE PORT-CHANNEL

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 9.0.2.0	Introduced on the S6000.
Version 9.0.0.0	Introduced on the Z9000.
Version 8.3.19.0	Introduced on the S4820T.
Version 8.3.8.0	Introduced on the S4810.

reload-type

Configure a switch to reload as a DHCP client in BMP mode with all ports configured for Layer 3 traffic or in Normal mode.

Syntax

```
reload-type [bmp | normal—reload {[auto—save {enable |
disable}] | [config-scr-download {enable | disable}] | [dhcp-
timeout minutes]| retry-count number | vendor-class-identifier
description]
```

Use the `disable bmp` command to stop the BMP process.

Parameters

bmp	(Default) Enable the BMP reload type. The system acts as a DHCP client and downloads the Dell Networking OS image, configuration and boot files from a specified DHCP server.
normal-reload	Enable the normal reload type and disable BMP reload type. The system retrieves the Dell Networking OS image and startup-configuration files from the flash after performing a reload.
auto-save	Configure the auto save option to save the downloaded configuration or script file. They are not saved by default. When auto save is configured, downloaded configurations are automatically saved to the startup configuration. Auto saving the downloaded configurations also requires enabling the **config-scr-download** parameter. Downloaded scripts are automatically saved to the autoexec script.
config-scr-download {enable}	(Optional.) Configure whether the configuration file must be downloaded from the DHCP/file servers (enable).
config-download {disable}	(Optional.) Configure if the downloaded file will not be downloaded from the DHCP/file servers.
dhcp-timeout *minutes*	(Optional) Configure the DHCP timeout (in minutes) after which the BMP reload stops. The range is from 0 to 50. If a range of 0 is entered, the timeout is 0 (no limit). The default is **disabled**. NOTE: Dell Networking recommends setting the value to 2 or higher.
retry-count *number*	Configure the number of times to retry loading the Dell Networking OS image and configuration download. The retry limit is 0–6. If the retry limit is 0, no retry is performed. The default is 0.
vendor-class-identifier *description*	(Optional) Enter a brief description for DHCP Option 60. Maximum is 64 characters long.

NOTE:

This parameter replaces the deprecated parameter **user-defined-string**.

Defaults

BMP

Switches running BMP reload in BMP mode as a DHCP client with all ports configured for Layer 3 traffic.

Command Modes

GLOBAL CONFIGURATION

Command History

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 9.2(0.0)	Introduced support for `vendor-class-identifier` that replaces deprecated parameter `user-defined-string` Also added support for `retry-count`.
Version 9.1(0.0)	Introduced on the Z9000. Updated the command mode from EXEC Privilege to GLOBAL CONFIGURATION. Updated the parameter from `jumpstart` to `bmp`. Added support for the `config-scr-download` and `user-defined-string` commands.
Version 8.3.19.0	Introduced on the S4820T.
Version 8.3.1.0	Introduced on the S4810.

Usage Information

For an initial setup, the `config-scr-download` parameter of the `reload-type` command is enabled. After the configuration file is successfully downloaded, the `config—scr-download` parameter is automatically disabled. You can enable it again using the `reload-type` command.

Set the Auto Configuration mode (BMP or Normal reload) using the `reload-type` command. Next, enter the `reload` command to reload the switch in the configured mode.

When a switch reloads in BMP mode, all ports, including the management port, are automatically configured as Layer 3 physical ports. The switch runs DHCP client on all interfaces. You can reconfigure the default startup configuration and DHCP timeout values.

If the switch attempts to contact a DHCP server and one is not found, it enters a loop while reloading in BMP mode. To interrupt the reload and boot up in Normal mode, enter the `stop bmp` command. The startup configuration is then loaded from the local flash on the switch.

To toggle between Normal and BMP Auto Configuration modes, use the `reload-type` command in BMP. Reload settings for Auto Configuration mode that you configure are stored in memory and retained for future reboots and BMP software upgrades. To reload the switch in the last configured mode: Normal reload or BMP mode, you can enter the `reload` command at any time.

Upgrade any configuration changes that have changed the NVRAM content by performing a reload on the chassis.

While BMP is on, the Dell Networking OS Command Line Reference Guide prompt changes to “Dell-BMP”.

Uplink Failure Detection (UFD)

Uplink failure detection (UFD) provides detection of the loss of upstream connectivity and, if you use this with network interface controller (NIC) teaming, automatic recovery from a failed link.

NOTE: In Standalone, VLT, and Stacking modes, the UFD group number is 1 by default and cannot be changed.

clear ufd-disable

Re-enable one or more downstream interfaces on the switch/router that are in a UFD-Disabled Error state so that an interface can send and receive traffic.

Syntax

```
clear ufd-disable {interface interface | uplink-state-group
group-id}
```

Parameters

interface *interface*	Specify one or more downstream interfaces. For *interface*, enter one of the following interface types: • Fast Ethernet: `fastethernet {slot/port | slot/ port-range}` • 1 Gigabit Ethernet: `gigabitethernet {slot/port | slot/ port-range}` • 10 Gigabit Ethernet: `tengigabitethernet {slot/ port |slot/ port-range}` • Port channel: `port-channel {1-512 | port-channel-range}` Where `port-range` and `port-channel-range` specify a range of ports separated by a dash (-) and/or individual ports/port channels in any order; for example: `gigabitethernet 1/1-2,5,9,11-12 port-channel 1-3,5`. A comma is required to separate each port and port-range entry.
uplink-state-group *group-id*	Re-enables all UFD-disabled downstream interfaces in the group. The valid group-id values are from 1 to 16.

Defaults

A downstream interface in a UFD-disabled uplink-state group is also disabled and is in a UFD-Disabled Error state.

Command Modes	CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.19.0	Introduced on the S4820T.
Version 8.3.12.0	Introduced on the S4810.
Version 8.4.2.3	Introduced on the S-Series S50.

Related Commands

- downstream — assigns a port or port-channel to the uplink-state group as a downstream interface.
- uplink-state-group — creates an uplink-state group and enables the tracking of upstream links.

debug uplink-state-group

Enable debug messages for events related to a specified uplink-state group or all groups.

Syntax

`debug uplink-state-group [group-id]`

To turn off debugging event messages, enter the `no debug uplink-state-group [group-id]` command.

Parameters

group-id	Enables debugging on the specified uplink-state group. The valid group-id values are from 1 to 16.

Defaults	none
Command Modes	EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.19.0	Introduced on the S4820T.

Version 8.3.12.0	Introduced on the S4810.
Version 8.4.2.3	Introduced on the S-Series S50.

Related Commands [clear ufd-disable](#) — re-enables downstream interfaces that are in a UFD-Disabled Error state.

description

Enter a text description of an uplink-state group.

Syntax `description text`

Parameters

text	Text description of the uplink-state group. The maximum length is 80 alphanumeric characters.

Defaults none

Command Modes UPLINK-STATE-GROUP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.19.0	Introduced on the S4820T.
Version 8.3.12.0	Introduced on the S4810.
Version 8.4.2.3	Introduced on the S-Series S50.

Example

```
Dell(conf-uplink-state-group-16)# description test
Dell(conf-uplink-state-group-16)#
```

Related Commands [uplink-state-group](#)— creates an uplink-state group and enables the tracking of upstream links.

downstream

Assign a port or port-channel to the uplink-state group as a downstream interface.

Syntax `downstream interface`

To delete an uplink-state group, enter the `no downstream interface` command.

Parameters

interface	Enter one of the following interface types: • Fast Ethernet: `fastethernet {`*`slot/port`*`	`*`slot/port-range`*`}` • 1 Gigabit Ethernet: `gigabitethernet {`*`slot/port`*`	`*`slot/port-range`*`}` • 10 Gigabit Ethernet: `tengigabitethernet {`*`slot/port`*` |`*`slot/port-range`*`}` • Port channel: `port-channel {`*`1-512`*`	`*`port-channel-range`*`}` Where `port-range` and `port-channel-range` specify a range of ports separated by a dash (-) and/or individual ports/port channels in any order; for example: `gigabitethernet 1/1-2,5,9,11-12 port-channel 1-3,5`. A comma is required to separate each port and port-range entry.

Defaults

none

Command Modes

UPLINK-STATE-GROUP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.19.0	Introduced on the S4820T.
Version 8.3.12.0	Introduced on the S4810.
Version 8.4.2.3	Introduced on the S-Series S50.

Usage Information

You can assign physical port or port-channel interfaces to an uplink-state group.

You can assign an interface to only one uplink-state group. Configure each interface assigned to an uplink-state group as either an upstream or downstream interface, but not both.

You can assign individual member ports of a port channel to the group. An uplink-state group can contain either the member ports of a port channel or the port channel itself, but not both.

Related Commands

- upstream— assigns a port or port-channel to the uplink-state group as an upstream interface.
- uplink-state-group — creates an uplink-state group and enables the tracking of upstream links.

downstream auto-recover

Enable auto-recovery so that UFD-disabled downstream ports in an uplink-state group automatically come up when a disabled upstream port in the group comes back up.

Syntax

```
downstream auto-recover
```

To disable auto-recovery on downstream links, use the `no downstream auto-recover` command.

Defaults

The auto-recovery of UFD-disabled downstream ports is enabled.

Command Modes

UPLINK-STATE-GROUP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.19.0	Introduced on the S4820T.
Version 8.3.12.0	Introduced on the S4810.
Version 8.4.2.3	Introduced on the S-Series S50.

Related Commands

- downstream— assigns a port or port-channel to the uplink-state group as a downstream interface.
- uplink-state-group — creates an uplink-state group and enables the tracking of upstream links.

downstream disable links

Configure the number of downstream links in the uplink-state group that are disabled if one upstream link in an uplink-state group goes down.

Syntax

```
downstream disable links {number |all}
```

To revert to the default setting, use the `no downstream disable links` command.

Parameters		
	number	Enter the number of downstream links to be brought down by UFD. The range is from 1 to 1024.
	all	Brings down all downstream links in the group.

Defaults No downstream links are disabled when an upstream link in an uplink-state group goes down.

Command Modes UPLINK-STATE-GROUP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.19.0	Introduced on the S4820T.
Version 8.3.12.0	Introduced on the S4810.
Version 8.4.2.3	Introduced on the S-Series S50.

Usage Information A user-configurable number of downstream interfaces in an uplink-state group are put into a link-down state with an UFD-Disabled error message when one upstream interface in an uplink-state group goes down.

If all upstream interfaces in an uplink-state group go down, all downstream interfaces in the same uplink-state group are put into a link-down state.

Related Commands

- downstream — assigns a port or port-channel to the uplink-state group as a downstream interface.
- uplink-state-group — creates an uplink-state group and enables the tracking of upstream links.

enable

Enable uplink state group tracking for a specific UFD group.

Syntax `enable`

To disable upstream-link tracking without deleting the uplink-state group, use the `no enable` command.

Defaults Upstream-link tracking is automatically enabled in an uplink-state group.

Command Modes

UPLINK-STATE-GROUP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.19.0	Introduced on the S4820T
Version 8.3.12.0	Introduced on the S4810.
Version 8.4.2.3	Introduced on the S-Series S50.

Related Commands

- uplink-state-group— creates an uplink-state group and enables the tracking of upstream links.

show running-config uplink-state-group

Display the current configuration of one or more uplink-state groups.

Syntax

`show running-config uplink-state-group [group-id]`

Parameters

group-id	Displays the current configuration of all uplink-state groups or a specified group. The valid group-id values are from 1 to 16.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.19.0	Introduced on the S4820T.
Version 8.3.12.0	Introduced on the S4810.

Version 8.4.2.3	Introduced on the S-Series S50.

Example

```
Dell#show running-config uplink-state-group
!
no enable
uplink state track 1
downstream GigabitEthernet 0/2,4,6,11-19
upstream TengigabitEthernet 0/48, 52
upstream PortChannel 1
!
uplink state track 2
downstream GigabitEthernet 0/1,3,5,7-10
upstream TengigabitEthernet 0/56,60
```

Related Commands

- show uplink-state-group — displays the status information on a specified uplink-state group or all groups.
- uplink-state-group — creates an uplink-state group and enables the tracking of upstream links.

show uplink-state-group

Display status information on a specified uplink-state group or all groups.

Syntax

`show uplink-state-group [group-id] [detail]`

Parameters

group-id	Displays status information on a specified uplink-state group or all groups. The valid group-id values are from 1 to 16.
detail	Displays additional status information on the upstream and downstream interfaces in each group

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.19.0	Introduced on the S4820T.
Version 8.3.12.0	Introduced on the S4810.
Version 8.4.2.3	Introduced on the S-Series S50.

Example

```
Dell# show uplink-state-group
Uplink State Group: 1 Status: Enabled, Up
Uplink State Group: 3 Status: Enabled, Up
Uplink State Group: 5 Status: Enabled, Down
Uplink State Group: 6 Status: Enabled, Up
Uplink State Group: 7 Status: Enabled, Up
Uplink State Group: 16 Status: Disabled, Up

Dell# show uplink-state-group 16
Uplink State Group: 16 Status: Disabled, Up

Dell#show uplink-state-group detail
(Up): Interface up (Dwn): Interface down (Dis): Interface
disabled
Uplink State Group     : 1 Status: Enabled, Up
Upstream Interfaces    :
Downstream Interfaces :

Uplink State Group     : 3 Status: Enabled, Up
Upstream Interfaces    : Gi 0/46(Up) Gi 0/47(Up)
Downstream Interfaces : Te 13/0(Up) Te 13/1(Up) Te 13/3(Up) Te
13/5(Up) Te 13/6(Up)

Uplink State Group     : 5 Status: Enabled, Down
Upstream Interfaces    : Gi 0/0(Dwn) Gi 0/3(Dwn) Gi 0/5(Dwn)
Downstream Interfaces : Te 13/2(Dis) Te 13/4(Dis) Te
13/11(Dis) Te 13/12(Dis) Te 13/13(Dis) Te 13/14(Dis) Te
13/15(Dis)

Uplink State Group     : 6 Status: Enabled, Up
Upstream Interfaces    :
Downstream Interfaces :

Uplink State Group     : 7 Status: Enabled, Up
Upstream Interfaces    :
Downstream Interfaces :

Uplink State Group     : 16 Status: Disabled, Up
Upstream Interfaces    : Gi 0/41(Dwn) Po 8(Dwn)
Downstream Interfaces : Gi 0/40(Dwn)
```

Related Commands

- show running-config uplink-state-group— displays the current configuration of one or more uplink-state groups.
- uplink-state-group — create an uplink-state group and enables the tracking of upstream links.

uplink-state-group

Create an uplink-state group and enable the tracking of upstream links on a switch/ router.

Syntax

`uplink-state-group` *`group-id`*

To delete an uplink-state group, enter the `no uplink-state-group group-id` command.

Parameters

group-id	Enter the ID number of an uplink-state group. The range is from 1 to 16.

Defaults

none

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.19.0	Introduced on the S4820T.
Version 8.3.12.0	Introduced on the S4810.
Version 8.4.2.3	Introduced on the S-Series S50.

Usage Information

After you enter the command, to assign upstream and downstream interfaces to the group, enter Uplink-State-Group Configuration mode.

An uplink-state group is considered to be operationally up if at least one upstream interface in the group is in the Link-Up state.

An uplink-state group is considered to be operationally down if no upstream interfaces in the group are in the Link-Up state. No uplink-state tracking is performed when a group is disabled or in an operationally down state.

To disable upstream-link tracking without deleting the uplink-state group, use the `no enable` command in uplink-state-group configuration mode.

Example

```
Dell(conf)#uplink-state-group 16
Dell(conf)#
02:23:17: %RPM0-P:CP %IFMGR-5-ASTATE_UP: Changed uplink state
group Admin state to up: Group 16
```

Related Commands

- show running-config uplink-state-group — displays the current configuration of one or more uplink-state groups.
- show uplink-state-group — displays the status information on a specified uplink-state group or all groups.

upstream

Assign a port or port-channel to the uplink-state group as an upstream interface.

Syntax

`upstream *interface*`

To delete an uplink-state group, use the `no upstream interface` command.

Parameters		
	interface	Enter one of the following interface types: • Fast Ethernet: `fastethernet {`*`slot/port`*` | `*`slot/port-range`*`}` • 1 Gigabit Ethernet: `gigabitethernet {`*`slot/port`*` | `*`slot/port-range`*`}` • 10 Gigabit Ethernet: `tengigabitethernet {`*`slot/port`*` | `*`slot/port-range`*`}` • 40 Gigabit Ethernet: `fortyGigE {`*`slot/port`*` | `*`slot/port-range`*`}` • Port channel: `port-channel {`*`1-512`*` | `*`port-channel-range`*`}` Where `port-range` and `port-channel-range` specify a range of ports separated by a dash (-) and/or individual ports/port channels in any order; for example: `gigabitethernet 1/1-2,5,9,11-12 port-channel 1-3,5`. A comma is required to separate each port and port-range entry.

Defaults none

Command Modes UPLINK-STATE-GROUP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.19.0	Introduced on the S4820T.
Version 8.3.12.0	Introduced on the S4810.
Version 8.4.2.3	Introduced on the S-Series S50.

Usage Information

You can assign physical port or port-channel interfaces to an uplink-state group.

You can assign an interface to only one uplink-state group. Configure each interface assigned to an uplink-state group as either an upstream or downstream interface, but not both.

You can assign individual member ports of a port channel to the group. An uplink-state group can contain either the member ports of a port channel or the port channel itself, but not both.

Example

```
Dell(conf-uplink-state-group-16)# upstream gigabitethernet
1/10-15
Dell(conf-uplink-state-group-16)#
```

Related Commands

- downstream — assigns a port or port-channel to the uplink-state group as a downstream interface.
- uplink-state-group — creates an uplink-state group and enables the tracking of upstream links.

Simple Network Management Protocol (SNMP) and Syslog

This chapter contains commands to configure and monitor the simple network management protocol (SNMP) v1/v2/v3 and Syslog.

The chapter contains the following sections:

- SNMP Commands
- Syslog Commands

SNMP Commands

The following SNMP commands are available in the Dell Networking operating software.

The simple network management protocol (SNMP) is used to communicate management information between the network management stations and the agents in the network elements. Dell Networking OS supports SNMP versions 1, 2c, and 3, supporting both read-only and read-write modes. Dell Networking OS sends SNMP traps, which are messages informing an SNMP management system about the network. Dell Networking OS supports up to 16 SNMP trap receivers.

Important Points to Remember

- Typically, 5-second timeout and 3-second retry values on an SNMP server are sufficient for both LAN and WAN applications. If you experience a timeout with these values, the recommended best practice on Dell Networking switches (to accommodate their high port density) is to increase the timeout and retry values on your SNMP server to the following:
  - SNMP Timeout — greater than 3 seconds.
  - SNMP Retry count — greater than 2 seconds.
- If you want to query an E-Series switch using SNMP v1/v2/v3 with an IPv6 address, configure the IPv6 address on a non-management port on the switch.
- If you want to send SNMP v1/v2/v3 traps from an E-Series using an IPv6 address, use a non-management port.
- SNMP v3 informs are not currently supported with IPv6 addresses.
- If you are using access control lists (ACLs) in an SNMP v3 configuration, group ACL overrides user ACL if the user is part of that group.
- SNMP operations are not supported on a virtual local area network (VLAN).

snmp-server enable traps

Enable SNMP traps.

Syntax

`snmp-server enable traps [notification-type] [notification-option]`

To disable traps, use the `no snmp-server enable traps [notification-type] [notification-option]` command.

Parameters

notification-type	Enter the type of notification from the following list: • `bgp` — Notification of changes in the BGP process. • `config` — Notification of changes to the startup or running configuration. • `ecfm` — Notification of changes to ECFM. • `ecmp` — Enable an ECMP trap to notify of ECMP or link bundle traffic imbalances. • `envmon` — For Dell Networking device notifications when an environmental threshold is exceeded. • `isis` — Notification of intermediate service traps. • `lacp` — Notification of changes. • `snmp` — Notification of RFC 1157 traps. • `stp` — Notification of a state change in the spanning tree protocol (RFC 1493). • `vlt` — Notification of virtual link trunking. • `vrrp` — Notification of a state change in a VRRP group. • `xstp` — Notification of a state change in MSTP (802.1s), RSTP (802.1w), and PVST+.
notification-option	For the `envmon` notification-type, enter one of the following optional parameters: • `cam-utilization` • `fan` • `supply` • `temperature` For the `snmp` notification-type, enter one of the following optional parameters: • `authentication` • `coldstart` • `linkdown` • `linkup`

Defaults

Not enabled.

Command Modes	CONFIGURATION
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*. The following is a list of the Dell Networking OS version history for this command.

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 9.1(0.0)	Added support for copy-config and ecmp traps.
Version 8.3.19.0	Introduced on the S4820T.
Version 8.3.11.1	Introduced on the Z9000.
Version 8.3.7.0	Introduced on the S4810.
Version 8.4.1.0	Added support for VRRP traps.
Version 7.6.1.0	Added support for STP and xSTP traps. Introduced on the S-Series.
Version 7.5.1.0	Introduced on the C-Series.
E-Series legacy command	

Usage Information

Dell Networking OS supports up to 16 SNMP trap receivers.

If you do not configure this command, no traps controlled by this command are sent. If you do not specify a `notification-type` and `notification-option`, all traps are enabled.

snmp-server host

Configure the recipient of an SNMP trap operation.

Syntax

`snmp-server host ip-address | ipv6-address`

To remove the SNMP host, use the `no snmp-server host ip-address` command.

Parameters

ip-address	Enter the keyword `host` then the IP address of the host (configurable hosts is limited to 16).
ipv6-address	Enter the keyword host then the IPv6 address of the host in the x:x:x:x::x format. NOTE: The :: notation specifies successive hexadecimal fields of zero.

traps	(OPTIONAL) Enter the keyword `traps` to send trap notifications to the specified host. The default is **traps**.
informs	(OPTIONAL) Enter the keyword `informs` to send inform notifications to the specified host. The default is **traps**.
version 1 | 2c | 3	(OPTIONAL) Enter the keyword version to specify the security model then the security model version number `1`, `2c`, or `3`: - Version `1` is the least secure version. - Version `3` is the most secure of the security modes. - Version `2c` allows transmission of informs and counter 64, which allows for integers twice the width of what is normally allowed. The default is version **1**.
auth	(OPTIONAL) Enter the keyword `auth` to specify authentication of a packet without encryption.
noauth	(OPTIONAL) Enter the keyword `noauth` to specify no authentication of a packet.
priv	(OPTIONAL) Enter the keyword `priv` to specify both authentication and then scrambling of the packet.
community-string	Enter a text string (up to 20 characters long) as the name of the SNMP community. NOTE: For version 1 and version 2c security models, this string represents the name of the SNMP community. The string can be set using this command; however, Dell Networking OS recommends setting the community string using the `snmp-server community` command before executing this command. For version 3 security model, this string is the USM user security name.
udp-port *port-number*	(OPTIONAL) Enter the keywords `udp-port` followed by the port number of the remote host to use. The range is from 0 to 65535. The default is **162**.
notification-type	(OPTIONAL) Enter one of the following keywords for the type of trap to be sent to the host: - `bgp` — Enable BGP state change traps. - `ecfm` — Enable ECFM state change traps. - `entity` — Enable entity change traps. - `envmon` — Enable SNMP environmental monitor traps. - `eoam` — Enable EOAM state change traps - `ets` — Enable ets traps - `fips` — Enable FIP Snooping state change traps - `lacp` — Enable LACP state change traps.

- `isis` — Enable ISIS adjacency change traps
- `pfc` — Enable pfc traps
- `snmp` — Enable SNMP trap
- `stp` — Enable 802.1d state change traps
- `vlt` — Enable VLT traps
- `vrrp` — Enable VRRP state change traps
- `xstp` — Enable 802.1s, 802.1w, and PVST+ state change traps

The default is all trap types are sent to host.

Defaults As above.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 9.1(0.0)	Added support for config and ecmp traps.
Version 8.3.19.0	Introduced on the S4820T.
Version 8.3.11.1	Introduced on the Z9000.
Version 8.3.7.0	Introduced on the S4810.
Version 8.4.1.0	Added support for VRRP traps.
Version 7.6.1.0	Added support for STP and xSTP notification types. Introduced on the S-Series.
Version 7.5.1.0	Introduced on the C-Series.
E-Series legacy command	

Usage Information In order to configure the router to send SNMP notifications, enter at least `one snmp-server host` command. If you enter the command with no keywords, all trap types are enabled for the host. If you do not enter an `snmp-server host` command, no notifications are sent.

In order to enable multiple hosts, issue a separate `snmp-server host` command for each host. You can specify multiple notification types in the command for each host.

When multiple `snmp-server host` commands are given for the same host and type of notification (trap or inform), each succeeding command overwrites the previous command. Only the last `snmp-server host` command will be in effect. For example, if you enter an `snmp-server host inform` command for a host and then enter another `snmp-server host inform` command for the same host, the second command replaces the first command.

The `snmp-server host` command is used with the `snmp-server enable` command. Use the `snmp-server enable` command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one `snmp-server enable` command and the `snmp-server host` command for that host must be enabled.

NOTE: For v1 / v2c trap configuration, if the community-string is not defined using the `snmp-server community` command prior to using this command, the default form of the `snmp-server community` command automatically is configured with the community-name the same as specified in the `snmp-server host` command.

Configuring Informs

To send an inform, use the following steps:

1. Configure a remote engine ID.
2. Configure a remote user.
3. Configure a group for this user with access rights.
4. Enable traps.
5. Configure a host to receive informs.

Related Commands	snmp-server enable traps — enables SNMP traps.

Syslog Commands

The following commands allow you to configure logging functions on all Dell Networking switches.

clear logging

Clear the messages in the logging buffer.

Syntax	`clear logging`
Defaults	none
Command Modes	EXEC Privilege
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.

Version 8.3.19.0	Introduced on the S4820T.
Version 8.3.11.1	Introduced on the Z9000.
Version 8.3.7.0	Introduced on the S4810.
Version 7.6.1.0	Introduced on the S-Series.
Version 7.5.1.0	Introduced on the C-Series.
E-Series legacy command	

Related Commands

show logging — displays logging settings and system messages in the internal buffer.

logging

Configure an IP address or host name of a Syslog server where logging messages are sent. Multiple logging servers of both IPv4 and/or IPv6 can be configured.

Syntax

```
logging {ip-address | ipv6-address | hostname} [vrf vrf-name]
```

To disable logging, use the `no logging` command.

Parameters

ip-address	Enter the IPv4 address in dotted decimal format.
ipv6-address	Enter the IPv6 address in the x:x:x:x::X format. NOTE: The :: notation specifies successive hexadecimal fields of zeros.
hostname	Enter the name of a host already configured and recognized by the switch.

Defaults

Disabled.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.19.0	Introduced on the S4820T.
Version 8.3.11.1	Introduced on the Z9000.
Version 8.3.7.0	Introduced on the S4810.

Version 8.4.1.0	Added support for IPv6.
Version 7.6.1.0	Introduced on the S-Series.
Version 7.5.1.0	Introduced on the C-Series.
E-Series legacy command	

Usage Information

Multiple logging servers of both IPv4 and/or IPv6 can be configured.

Related Commands

[logging trap]() — enables logging to the Syslog server based on severity.

logging buffered

Enable logging and specify which messages are logged to an internal buffer. By default, all messages are logged to the internal buffer.

Syntax

`logging buffered [level] [size]`

To return to the default values, use the `default logging buffered` command.

To disable logging stored to an internal buffer, use the `no logging buffered` command.

Parameters

level	(OPTIONAL) Indicate a value from 0 to 7 or enter one of the following equivalent words: `emergencies`, `alerts`, `critical`, `errors`, `warnings`, `notifications`, `informational`, or `debugging`. The default is **7** or **debugging**.
size	(OPTIONAL) Indicate the size, in bytes, of the logging buffer. The number of messages buffered depends on the size of each message. The range is from 40960 to 524288. The default is **40960 bytes**.

Defaults

level = **7**; size = **40960 bytes**

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 9.0.2.0	Introduced on the S6000.

Version 8.3.19.0	Introduced on the S4820T.
Version 8.3.11.1	Introduced on the Z9000.
Version 8.3.7.0	Introduced on the S4810.
Version 7.6.1.0	Introduced on the S-Series.
Version 7.5.1.0	Introduced on the C-Series.
E-Series legacy command	

Usage Information

When you decrease the buffer size, all messages stored in the buffer are lost. Increasing the buffer size does not affect messages stored in the buffer.

Related Commands

clear logging — clears the logging buffer.

show logging — displays the logging setting and system messages in the internal buffer.

logging console

Specify which messages are logged to the console.

Syntax

`logging console [level]`

To return to the default values, use the `default logging console` command.

To disable logging to the console, use the `no logging console` command.

Parameters

level	(OPTIONAL) Indicate a value from 0 to 7 or enter one of the following parameters: `emergencies`, `alerts`, `critical`, `errors`, `warnings`, `notifications`, `informational`, or `debugging`. The default is **7** or **debugging**.

Defaults

level = **7**; size = **debugging**

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 8.3.19.0	Introduced on the S4820T.
Version 8.3.11.1	Introduced on the Z9000.

Version 8.3.7.0	Introduced on the S4810.
Version 7.6.1.0	Introduced on the S-Series.
Version 7.5.1.0	Introduced on the C-Series.
E-Series legacy command	

Related Commands

clear logging — clears the logging buffer.

show logging — displays the logging setting and system messages in the internal buffer.

logging monitor

Specify which messages are logged to Telnet applications.

Syntax

`logging monitor [level]`

To disable logging to terminal connections, use the `no logging monitor` command.

Parameters

level	Indicate a value from 0 to 7 or enter one of the following parameters: `emergencies`, `alerts`, `critical`, `errors`, `warnings`, `notifications`, `informational`, or `debugging`. The default is **7** or **debugging**.

Defaults

7 or **debugging**

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 9.0.2.0	Introduced on the S6000.
Version 8.3.19.0	Introduced on the S4820T.
Version 8.3.11.1	Introduced on the Z9000.
Version 8.3.7.0	Introduced on the S4810.
Version 7.6.1.0	Introduced on the S-Series.
Version 7.5.1.0	Introduced on the C-Series.

logging source-interface

Specify that the IP address of an interface is the source IP address of Syslog packets sent to the Syslog server.

Syntax

`logging source-interface interface`

To disable this command and return to the default setting, use the `no logging source-interface` command.

Parameters

interface	Enter the following keywords and slot/port or number information: • For a 100/1000 Ethernet interface, enter the keyword `GigabitEthernet` then the slot/port information. • For Loopback interfaces, enter the keyword `loopback` then a number from zero (0) to 16383. • For the management interface on the RPM, enter the keyword `ManagementEthernet` then the slot/port information. The slot range is from 0 to 1 and the port range is 0. • For a Port Channel interface, enter the keywords `port-channel` then a number. Tthe range is from 1 to 128. • For a ten-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 9.0.2.0	Introduced on the S6000.
Version 8.3.19.0	Introduced on the S4820T.
Version 8.3.11.1	Introduced on the Z9000.
Version 8.3.7.0	Introduced on the S4810.
Version 8.5.1.0	Added support for 4-port 40G line cards on ExaScale.

Version 7.6.1.0	Introduced on the S-Series.
Version 7.5.1.0	Introduced on the C-Series.
E-Series legacy command	

Usage Information

Syslog messages contain the IP address of the interface used to egress the router. By configuring the `logging source-interface` command, the Syslog packets contain the IP address of the interface configured.

Related Commands

logging— enables logging to the Syslog server.

show logging

Display the logging settings and system messages logged to the internal buffer of the switch.

Syntax

```
show logging [number | history [reverse][number] | reverse
[number] | summary]
```

Parameters

number	(OPTIONAL) Enter the number of messages displayed in the output. The range is from 1 to 65535.
history	(OPTIONAL) Enter the keyword `history` to view only information in the Syslog history table.
reverse	(OPTIONAL) Enter the keyword `reverse` to view the Syslog messages in FIFO (first in, first out) order.
summary	(OPTIONAL) Enter the keyword `summary` to view a table showing the number of messages per type and per slot. Slots *7* and *8* represent RPMs.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 9.0.2.0	Introduced on the S6000.
Version 8.3.19.0	Introduced on the S4820T.
Version 8.3.11.1	Introduced on the Z9000.
Version 8.3.7.0	Introduced on the S4810.

Version 7.6.1.0	Introduced on the S-Series.
Version 7.5.1.0	Introduced on the C-Series.
E-Series legacy command	

Example (Partial)

```
Dell#show logging
Syslog logging: enabled
    Console logging: level debugging
    Monitor logging: level debugging
    Buffer logging: level debugging, 5604 Messages Logged,
Size (524288 bytes)
    Trap logging: level informational
Oct 8 09:25:37: %RPM1:RP1 %BGP-5-ADJCHANGE: Connection with
neighbor 223.80.255.254 closed. Hold time
expired
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor
192.200.13.2 Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor
192.1.1.13 Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 1.1.14.2
Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor
192.1.1.14 Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 1.1.11.2
Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 192.1.1.5
Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 192.4.1.3
Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 192.1.1.4
Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 192.1.1.6
Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor
192.1.1.12 Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor
192.1.1.15 Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 192.1.1.3
Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor
192.200.12.2 Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 1.1.10.2
Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Session closed by
neighbor 1.1.10.2 (Hold time expired)
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor
192.200.14.7 Up
Oct 8 09:26:25: %RPM1:RP1 %BGP-5-ADJCHANGE: Connection with
neighbor 1.1.11.2 closed. Neighbor recycled
Oct 8 09:26:25: %RPM1:RP1 %BGP-5-ADJCHANGE: Connection with
neighbor 1.1.14.2 closed. Neighbor recycled
--More--
```

Example (History)

```
Dell#show logging history
Syslog History Table: 1 maximum table entries,
saving level Warnings or higher
  SNMP notifications not Enabled
```

```
%RPM:0:0 %CHMGR-2-LINECARDDOWN - Line card 3 down - IPC timeout
Dell#
```

show logging driverlog stack-unit

Display the driver log for the specified stack member.

Syntax	`show logging driverlog stack-unit unit#`

Parameters

stack-unit *unit#*	Enter the keywords `stack-unit` followed by the stack member ID of the switch for which you want to display the driver log. The range is from 0 to 7.

defaults: none

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 9.0.2.0	Introduced on the S6000.
Version 8.3.19.0	Introduced on the S4820T.
Version 8.3.11.1	Introduced on the Z9000.
Version 8.3.7.0	Introduced on the S4810.
Version 7.6.1.0	Introduced on the S-Series.

Usage Information

This command displays internal software driver information, which may be useful during troubleshooting switch initialization errors, such as a downed Port-Pipe.

terminal monitor

Configure the Dell Networking OS to display messages on the monitor/terminal.

Syntax

`terminal monitor`

To return to default settings, use the `terminal no monitor` command.

defaults: Disabled.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version 9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
Version 9.0.2.0	Introduced on the S6000.
Version 8.3.19.0	Introduced on the S4820T.
Version 8.3.11.1	Introduced on the Z9000.
Version 8.3.7.0	Introduced on the S4810.
Version 7.6.1.0	Introduced on the S-Series.
Version 7.5.1.0	Introduced on the C-Series.
E-Series legacy command	

Related Commands

logging monitor— sets the logging parameters on the monitor/terminal.